

iNCISIVE™

**Customer Guide to
INCISIVE Support**

9 September 2013

Welcome to INCISIVE Support

What's in this guide
Getting the latest information
Accessing the INCISIVE Support website
Report a defect or an enhancement idea
Customer Service Resources

This guide is intended to help you leverage the product and services provided by our Support representatives. It outlines the support available for our products and how to access that support.

We are committed to continually improving our process and providing on-going support for you. This guide is regularly updated; we encourage you to visit our website for the latest updates to product and service information, documentation, and other product resources.

What's in this guide

- For products and available services, see "Service levels and policies"
- On methods to contact Support, see "Customer Service resources"
- For help determining the type and severity of the problem and which support resources to use, see "3-Tier priority system"
- For steps you can take to resolve a problem before contacting INCISIVE Support, see "Before you contact INCISIVE Support..."
- For the problem resolution process we use when you call, see "Connecting with a INCISIVE Support Engineer"
- For what to do when your expectations are not met, see "Escalating incidents, defects, or enhancements"
- For instructions on submitting and following-up on defect reports and enhancement requests, see "Submitting defects and enhancements"

Getting the latest information

Our Support website contains the latest, downloadable versions of all documentation for our INCISIVE products. The most current version of this guide is always available on our Support website.

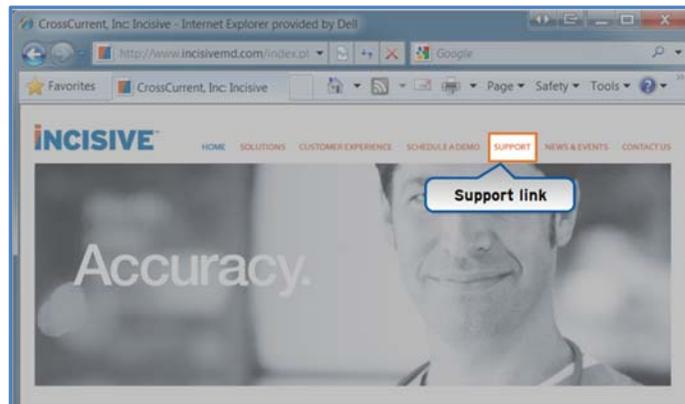
The INCISIVE product support website allows you to:

- View the latest product news, documentation, and other coding resources
- Download computer-based training and sign-up for web training seminars

- Review known issues with the software
- Join an email list and receive email newsletters on topics related to product support, updates, features under development, and technical alerts

Accessing the INCISIVE Support website

You can access our Support website at www.incisivemd.com. Click Support above the photo to view our support web page.



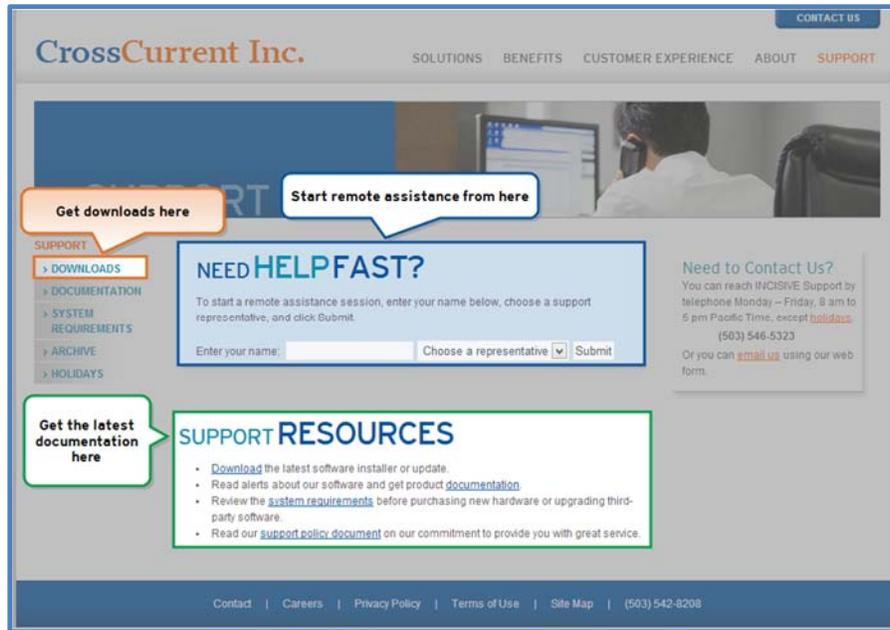
Our support page provides a single stop to get our latest software downloads, documentation, and getting help.

No Login Needed for Software Downloads

You no longer need a login to download our software. Simply go to the **DOWNLOADS** webpage and get the files you need.

1. Go the INCISIVE Support webpage.
2. Under the left column Support heading, click **DOWNLOADS**.

You can also get to the **DOWNLOADS** webpage by clicking on the Downloads link under the Support **RESOURCES** heading.



From the Software DOWNLOADS webpage, you will find our latest INCISIVE MD Installer, Update, Install Instructions, and Release Notes. If you have previously installed INCISIVE MD, you only need to download the much smaller Update file. Use the Install Instructions for steps in using either the Installer or Update file.

-
- ① You will need your encrypted provisioning file to complete your install. If you do not have your clinic's provisioning file, please contact INCISIVE Support to get it and help with completing your installation of INCISIVE MD.
-

Report a defect or an enhancement idea

To report a product defect or provide us with your INCISIVE product enhancement idea, use the Product Feedback Form on the Support website.

1. Go the INCISIVE Support webpage.
2. Under the right-side **Need to Contact Us?** heading, click the email us link.
3. Enter your contact information and your suggestion, product enhancement idea, or any other comment or concern you would like us to know.

Customer Service Resources

Department	Telephone / Fax	Email	Website
Customer Service	Voice: (503) 546-5323	support@incisivemd.com	http://www.incisivemd.com/support
Sales	Fax: (866) 899-2746	sales@incisivemd.com	http://www.incisivemd.com

You can contact us by phone, fax, email, or directly from our Support website. Please use the method that is most convenient for you.

Support Representatives

Support Representatives offer an array of technical skills. Some team members are operating system software certified, and all have expertise in our products, databases, operating systems software, and other related application software products.

Support Representatives can answer your questions about how to use our software and help you solve any problems you experience with its use. They can also refer you to our accounting personnel to talk about your monthly subscription billing issues, provide updated billing statements, or provide answer any other questions regarding your account with CrossCurrent.

INCISIVE Support Newsletter

Subscribe to the monthly INCISIVE Support email newsletter and watch for notifications about INCISIVE products. We use this newsletter to send important product information and updates regarding:

- Workflow and usability suggestions
- Frequently asked questions and answers
- Hot technical topics
- Web update announcements
- Lessons learned from customer implementations

ⓘ Remember to add support@crosscurrentinc.com to your safe sender list!

Support and Corporate Websites

Visit our corporate website for company press releases, investor information, and products and services we offer. The support website provides direct access to documentation, support, product forums, and training information.

Experience Level Promise

Service Description

Customer Performance Expectations

CrossCurrent Production Goals

Our performance, availability, and maintenance levels summarized here are subject to the terms and conditions of your product Business Associate, Contract and License, Support Agreements, and applicable law.

Service Description

CrossCurrent provides its software as an affordable hybrid software-as-service model. INCISIVE software client applications are installed on customer's workstations and laptops and the corresponding backend database and web servers are housed at our data center. Inter-connectivity between INCISIVE client applications and the backend servers use strong encryption standards when communicating over the Internet. We perform all database management and infrastructure maintenance for the INCISIVE software provided to our customers as part of their License and Support agreements.

Affordable Solution

We have to balance our customers' tolerance for downtime with the cost of providing available uptime. These two goals are diametrically opposed to each other, since guaranteeing greater uptime requires more equipment and people. In trying to reach an affordable balance between these goals, we are guided by two principles:

- No loss of data
- Patient data is secure during transport, storage, and use

Tier 2 INCISIVE Data Center

As defined by the Uptime Institute, a New Mexico-based information technology think tank and professional services organization, our Tier 2 data center requires:

- Single non-redundant distribution path serving the data center equipment
- Non-redundant capacity components
- Basic site infrastructure guaranteeing 99.741% availability

99.741% availability means less than 2 hours of downtime per year

Our data center is housed at [Infinity Internet](#), a carrier-grade co-location facility in downtown Portland, Oregon. This facility boasts the following physical specifications:

- 24x7 monitoring of all power, data, and security
- Seismically reinforced physical architecture
- Redundant HVAC environmental control systems
- UPS backup for all systems with standby 750 kilowatt generator
- Premise security provided via card lock and physical key combination
- OC-12 and OC-48 redundant fiber optic connections to the Internet

Customer Performance Expectations

Because we have assumed the burden of managing the INCISIVE web and database servers for our customers, we have housed them at our data center. Customers can rest assured knowing that we are doing our work in a professional manner and safeguarding their data according to applicable law and their License and Support agreements.

General Customer Experience Expectations

What do our customers want from our software? The feedback we have received indicates that they want simply to use software that just works and is available anytime they need it. This is a tall order but one in which we consistently strive to meet.

No Application Problems

We have a rigorous quality assurance testing process for our software products to minimize the potential software glitches. As with all software, we cannot completely eliminate problems our customer may encounter with our software because we do not control their computer environment. Potential problems can include conflicting installed applications and virus and malware threats. Our commitment to you is that when we are informed of a problem that we will diligently support you in resolving the matter to the best of our ability.

Always on

With our Tier 2 data center and the redundant systems in place, we can commit to providing you access to our INCISIVE servers every business day. We will schedule normal maintenance procedures on these systems after 5:00 pm Pacific Time weekdays and weekends. We will notify affected customers before changes are implemented if maintenance is done during regular business hours.

Competent Employees

We will provide competent personnel with the necessary skills and experience to provide our INCISIVE products and services to you. If however, in a customer's reasonable opinion, any of our personnel fail to carry out the services with sufficient competency, you may notify us. We will endeavor to rectify or remediate the situation as soon as is reasonably possible.

Business Continuity

We have written a disaster recovery plan and regularly test parts of that plan to ensure we have the ability to return to normal business operations within 2 weeks in the unlikely happening of a *force majeure* event.

Internet Connectivity

While we strive to meet all our customers' expectations, we are not responsible for the performance of their Internet service provider or Internet connection. In determining a customer's Internet connectivity requirements, the latency between our data center and the customers' workstations and laptops is more important than the availability of bandwidth. Customer should review the *Recommended Hardware and Software Recommendations* documents for each INCISIVE software product for the specific Internet connectivity requirements for that product.

Wireless Caveat. Due to the occasional intermittent nature and low throughput of wireless connectivity, a customer's experience in using INCISIVE software may degrade to the point where an application operates very slowly or frequently loses connection with to its INCISIVE server. We recommend for users using our INCISIVE software consistently throughout the day that they be connected to the Internet with a hardwire connection.

Service Restoration

Depending on the INCISIVE product used by our customers, non-maintenance disruptions in service or poor Internet connectivity may affect a customer's workflow and business operations differently. Business criticality also plays a part in that not all INCISIVE software is required to manage the clinic on daily basis. When service is disrupted, for whatever reason, we will endeavor to restore access to our various INCISIVE products according to the table below.

INCISIVE Product	Description	Return to Service Level
MD	Surgical planning and payment auditing software	1 business day
PM	Practice management software for storing patient demographics, physician patient schedules, and charge and payment entry	4 hours during normal business hours or the next business day
IQ	Web reports portal	3 business days
IS	Data extraction and integration software to retrieve patient demographics and claim payment information from customers' practice management systems	2 business days

In the event of a cataclysmic earthquake, meteorite strike, zombie attack, or any other *force majeure* event in which the city of Portland lay in ruins or chaos, our business continuity plan calls for the restoration of service to our customers within 2 weeks of the event.

Customer Notification

We will contact affected customers either by phone, instant message, in-application message, or email before implementing a change. For planned maintenance changes, notification will occur 3 business days before the change is implemented. The notification will be to the primary clinic or technical contact and will indicate which product will be affected and the date and time of the expected outage.

For emergency changes, every effort will be made to contact customers before the change is made. Given the nature of an emergency change, we have to balance customer notification with ensuring we maintain our two guiding principles. With the completion of any emergency change, CrossCurrent will notify affected customers within the next business day by email or in-application message.

CrossCurrent Production Goals

CrossCurrent does not have any performance penalties written into our contracts or License and Support agreements. We have found these to be counterproductive to building a relationship with our customers. CrossCurrent takes it as a matter of personal pride to provide our customers with 99.741% availability to our INCISIVE software.

Maintenance and Service Changes

In order to meet customers' performance expectations and our own internal production goals, the INCISIVE servers require regularly scheduled operating system and infrastructure software maintenance. During periods where maintenance is being performed, limited or no availability may occur to our software. Depending on the INCISIVE software being used, customers will receive different notifications of server unavailability.

- MD — On the INCISIVE MD login, a maintenance message will be displayed.
- PM — A logged in user will receive an administrator console message about disconnecting the user. For an INCISIVE PM user not logged on, when attempting to log in the server will report an error message about not being able to connect.
- IQ — When the web reports portal is unavailable, the customer will be redirected to a web page providing details about the unavailability of the portal and any detail relevant to the outage

Because we cannot control the release of operating system updates, we do not publish a maintenance calendar. When operating system or hardware maintenance needs to occur, it tends to require either taking a server offline or rebooting the server after maintenance is complete. In these situations, all INCISIVE product customers may be affected and we will use the normal customer notification process.

Hardware Failures and Emergency Maintenance

We have a hardware monitoring system in place to better manage the eventual failure of server hardware components. In many cases, these types of hardware failures are catastrophic in nature in that they occur almost instantaneous and cause the unavailability of the affected server. To account for these situations, we have provisioned redundant secondary servers for all key data center systems.

Other situations occur where immediate software maintenance needs to be done on the recommendation of Microsoft or other third-party vendor in order to preserve security or prevent a potential software issue. In these situations, CrossCurrent may not have the opportunity to inform all affected customers before the change occurs. In these instances where notification may not occur before the implemented change, CrossCurrent will notify affected customers within the next business day by email.

Three Level Backup

To minimize data loss, CrossCurrent does an incremental transactional backup of all INCISIVE databases every 15 minutes. This ensures that in case of data loss or corruption, transactional data can be restored with a maximum time of loss of 15 minutes. Normal data backup procedures typically ensure only a maximum time of loss of 24 hours. As an additional level of backup and security, all data is stored on a secure secondary backup server and encrypted with 2048-bit encryption. As a third level of backup protection, the encrypted data is stored off-site with Amazon Simple Storage Service (S3).

Safeguarding Protected Health Information

HIPAA and HITECH Compliance

Passwords

Breach of Protected Information

To meet our regulatory obligations to safeguard protected health information (PHI), we have completed an extensive security review, enhanced the security of the INCISIVE Data Center, and provided additional security management within the INCISIVE applications.

HIPAA and HITECH Compliance

As with any other healthcare software vendor, we worked with our customers to enable them to be compliant with the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191. With the passage of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") as part of the American Recovery and Reinvestment Act of 2009 (ARRA), Public Law 111-5, certain provisions of HIPAA that previously only applied to our customers now pertain directly to CrossCurrent. With this change, we have upgraded our facilities and internal business processes to comply with the requirements of the HITECH Act. Customers should refer to our BAA or HITECH BAA Amendment for specific details on our commitments to you mandated by HITECH.

Safeguarding PHI

Every day we are all reading about the breach of PHI or the hacking of a company's website. The measures needed for protecting information and thwarting computer attacks has increased many times over the last several years. We constantly review our procedures and hardware configurations based on the latest data loss or exploit. Additionally, we complete an annual security review of our policies and procedures.

Given the sensitive nature of our security policies and procedures, we will not distribute these to customers or vendors but will allow anyone to examine them as part of a compliance review. Contact INCISIVE Support and we will schedule a web conference to review our security policies and procedures by remote desktop sharing.

Security Review

We have completed an extensive security self-assessment based upon the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) 2011. The CSF is an information security framework that harmonizes the requirements of existing standards and regulations, including federal (HIPAA, HITECH), third party (PCI, COBIT) and government (NIST, FTC). The companion Information Security Implementation Manual contains extensive coverage of 13 security control categories comprised of 42

objectives and 135 specifications. The Manual provides us with the needed structure, detail, and clarity relating to information security tailored to the healthcare industry.

We suggest customers also use the CSF Implementation Manual as the baseline for their own self-assessments in meeting the requirements for HIPAA and HITECH. The CSF Implementation Manual can be downloaded from the [HITRUST Central website](#) after registering with HITRUST.

Data Center Security

For our customers' peace of mind and to satisfy our own paranoia, we have configured our Data Center infrastructure and procedures to provide:

- 24x7 monitoring of all data flows and security
- All INCISIVE servers are behind production class Juniper hardware and redundant Microsoft software firewalls
- Daily monitoring and automatic lock out of all unauthorized attempts to access any of our systems

Customer should review the *Recommended Hardware and Software Recommendations* documents for each INCISIVE software product for the specific inbound Internet ports needing to be configured for our products.

Application Security

All communication between INCISIVE client software installed on customers' workstations and laptops is secured to meet the following security specifications:

- All traffic is encrypted via 128-bit Secure Socket Layer (SSL) protocol layer and is initiated from within the clinic—*never from outside*.
- All transactions are identified and processed via a clinic-unique private 865-byte certificate and dependent clinic identifier.

Additionally, each of our applications, INCISIVE MD and INCISIVE PM, are configurable to set user permissions based upon assigned user groups and individual application features. This allows clinic administrators to set specific permissions for each user based upon their role within the clinic and the tasks performed by their roles. Refer to INCISIVE Support website Documentation section for the INCISIVE 3.6 Release Notes for security configuration instructions, or contact INCISIVE Support.

Email and File Sharing

We will not email or send PHI to customers or their billing service companies unencrypted. We have contracted with Microsoft to use their Hosted Encryption solution to send encrypted emails to our customers to send PHI or attachments with PHI within them. In rare circumstances, we may use a secondary method by sending unencrypted email that contains no PHI but attach an encrypted file with PHI. The password for the encrypted attachment will be communicated to the email receiver over the phone.

Passwords

We will never ask you for your password and you should never share your INCISIVE application password with another user.

Strong Passwords

Our INCISIVE software products enforce strong user passwords. From your initial temporary password to your regularly changed password, all passwords must be:

- Between 8 to 20 characters in length
- Must contain at least one upper case letter, lower case letter, a number, and special character like \$, #, %, *, or !
- Free of consecutive identical characters like "111" or "aaa"
- Have at least four characters changed when new passwords are created to prevent users from simply adding a character to an old password
- Not the same as a previously used password

Passwords may not contain a string of characters that are the same as a user's first name, last name, or their User Name.

Password Policies

The local administrator of your INCISIVE software can set a number of password policies to enforce basic industry standards for password management. Refer to each applications user guide for how to change these settings or contact INCISIVE Support.

- **Forced Password Changes.** The INCISIVE software can be set to force users to change their password on a regular basis. The frequency when passwords must be changed can be from never to 365 days. Our suggested setting for this policy is every 90 days. The default setting is to have this rule turned off (0 days).
- **Idle Time-out.** After 30 minutes of idle activity, the INCISIVE software will return a user to the login screen. This setting can be changed from 1 minute to 480 minutes. The default setting is 30 minutes.
- **User Lockout.** To prevent unauthorized attempts at gaining access to INCISIVE software, the number of failed logins can be set before a user account is locked out from logging in. The default for this setting is five failed attempts. Once an account is locked out, either the local administrator for INCISIVE software or an INCISIVE Support representative will be required to unlock the user's account.
- **Lockout Notice.** Once an account is locked out, an email will be sent to the user whose account is locked out as well as any other user designed by your local INCISIVE software administrator. The lock out email will provide the instructions on how a user can have their account unlocked.

Password Changes or Resetting

A user will receive their temporary password via an email from the INCISIVE MD server application. The user will need to change this password upon first login. Users have the ability to change their passwords at any time after logging into an INCISIVE application. To have a password reset, a user will need to contact either their local INCISIVE software administrator or INCISIVE Support to have their password reset. A temporary password

may be provided over the phone in rare circumstances when the identity of a caller can be confirmed. But the preferred method is to send the temporary password via email from INCISIVE Support.

Breach of Protected Information

To ensure against a breach of PHI to unauthorized individuals, we encrypt all storage media containing PHI, PHI sent over the Internet in emails and files, and certain information stored with INCISIVE software databases.

Breach Notification

If we inadvertently disclose or become aware of unencrypted PHI provided to someone not covered by HIPAA or HITECH, we will notify within 5 business days either the customer or the sender of the unencrypted PHI of the possible breach of HIPAA and HITECH security and privacy regulations. This notification will include:

- A description of the possible breach and when it was discovered
- Whose PHI was possibly disclosed
- Who were the recipients of the disclosure
- What protected information may have been disclosed
- What remediation steps we have taken regarding the possible breach

Incident Investigation

If we are the ones who possibly disclosed the PHI, our Security and Privacy Officer will conduct a Breach Incident Investigation to ascertain the details regarding the possible breach and work the appropriate individuals to recommended corrective actions. After completing the Breach Incident Investigation, we will take prompt and appropriate corrective action to rectify any deficiencies in our security procedures, policies, or training that resulted in the disclosure and implement any additional actions needed to prevent future disclosures.

Breach Exemptions

There are specific exemptions within the breach notification regulations when PHI is sent between a covered entity or business associate unencrypted that does not result in a disclosure of that PHI to an unintended party. If we receive PHI from a customer or their billing service company unencrypted, we will inform the customer that this does not meet the requirements of HIPAA/HITECH and request that future emails or files be encrypted and file an incident report with our corporate Security and Privacy Officer.

Customer Data and Reports

Data Extractions
INCISIVE IQ Web Reports Portal
Database Backup Media

As indicated in your INCISIVE Software Subscription Agreement, you own your data. In addition to querying and reporting capabilities within INCISIVE software, we also provide additional access to your data:

- **Data Extractions** — As the need arises, we can extract data from your INCISIVE Software database and provide it to you as a set of Microsoft Excel spreadsheets or text files.
- **INCISIVE IQ Web Reports Portal** — This is a secure Microsoft SQL Server Reporting website that is setup for each customer. The reports accessible to you on the web portal are based on the INCISIVE Software you license from us along with any we develop and deploy specifically for you.
- **Database Backup Media** — To accommodate the occasional need by customers to have a complete copy of their data, we can provide complete copies of your INCISIVE Software databases. We use Microsoft SQL Server as our database technology and will provide an encrypted backup file.

Data Extractions

For INCISIVE PM customers, we provide a basic query capability within the application that is limited to pulling information from single database tables. For queries that require more sophisticated SQL queries, users may request INCISIVE Support to create the query and extract the data for them. We will review the request and determine whether the data extraction is a routine request or outside the scope of INCISIVE Support. When the data extraction is outside the scope of your support, we will provide an estimate of the consulting cost required to create and deploy the requested data extraction according to your Professional Services Terms and Conditions Agreement.

In contrast to INCISIVE PM, INCISIVE MD has a limited reporting capability within the application. For customers of INCISIVE MD who desire data about their surgeries, disputes, contract details or other data contained in the system, we likely already have reports we can run for these specific needs; such as, a list of surgeries with diagnosis codes for professional certifications. For other types of common data requests, INCISIVE Support has many existing queries that can be run and securely sent to you. Please contact INCISIVE Support to determine the current list of available INCISIVE MD queries.

INCISIVE IQ Web Reports Portal

Reporting functions are available within INCISIVE client Software and via the INCISIVE IQ web reports portal. The report portal contains reports for commonly requested data and for sophisticated reports.

If you determine a need for a specific set of data not already available from a report within INCISIVE software, please contact INCISIVE Support. We will review the request and determine whether if the report is a routine request or one that beyond the scope of INCISIVE Support. If a web report is beyond the scope of our normal support, we will provide an estimate of the consulting cost required to create and deploy the needed report according to your Professional Services Terms and Conditions Agreement. We will usually ask customers to provide a Microsoft Excel spreadsheet that provides a mock-up of how they would like the report to be formatted.

We are happy to assist you in accessing your data but we cannot support other companies' products. Below are some examples of the assistance we do and do not provide as part of you support agreement.

Topics Covered	Topics Not Covered
"How do I" type questions	Creation of, or modification of, user created reports
Functionality and use of reports provided with INCISIVE Software	Modification of canned reports
Any situation where there is a known issue or potential issues with a report provided with INCISIVE Software	Design or setup of reports or data extractions using third-party tools
	Use of Microsoft Excel to manipulate report data

Database Backup Media

You may also request a complete copy of your INCISIVE Software database. We will encrypt the requested database and provide it to you as a no-cost secure download. If you require the database on physical media, you can provide your own or we will charge you for the cost of the media, insurance, and shipping. The media will be encrypted and sent by a recognized overnight express carrier (FedEx, UPS, or USPS) with signature confirmation.

While providing your data to you, we have a limited ability within INCISIVE Support to help you understand how CrossCurrent has created and maintained its INCISIVE software databases. The table below outlines the support topics we can assist you with and those not covered by INCISIVE Support. If you need help for those topics not covered, you may request consulting services from us as outlined in your Professional Services Agreement.

Topics Covered	Topics Not Covered
Restoring and accessing database media backups	Training or tutorials on the INCISIVE Software database schemas
"How do I" type questions	Design or detailed configuration of customer databases

Topics Covered	Topics Not Covered
Suggestions on source of reconciliation difficulties	Performing reconciliation of external reports with INCISIVE software
Unencrypting database media backups	
Use of CrossCurrent download websites	

Support level and policies

Support Levels
CrossCurrent Support Policy
Third-party software and support policies

The support policies and service summarized here are subject to the terms and conditions of your product License and Support agreements.

Support Levels

CrossCurrent, Inc. offers two levels of service for INCISIVE products:

- **Regular Support Plan** — This is the basic plan that offers unlimited calls to a Support Representative during regular business hours: 8:00 am to 5:00 pm Pacific Time, Monday – Friday, except holidays.
- **After Hours Option** — Add this option when you need occasional support after regular support hours. You only pay for the calls you make during non-business hours or on weekends.

Support Plan Features

Feature	Regular Support Plan	After Hours Option
Number of calls accepted	Unlimited	As pre-arranged
Remote assistance support	Yes	Yes
24 x 7 fax and voice mail access	Yes	Yes
Access to password protected INCISIVE Support Website	Yes	Yes
Support Hours	8:00 am to 5 pm Pacific Time, Monday – Friday	As requested

① You must purchase the After Hours Option before the date needed.

CrossCurrent Holidays

CrossCurrent company holidays for the current year are posted on the INCISIVE Support website. These federal holidays are commonly observed:

Martin Luther King Day	New Year's Eve and New Year's Day
Memorial Day	Independence Day
Labor Day	Thanksgiving Day and the day after
	Christmas Eve and Christmas Day

On these days, Regular Support Plan customers will need to pre-arrange an After Hours Option if they need to call for support.

Support Response Times

Customer Service response times for questions, issues, and defects reported during regular business hours are as follows. Refer to the Three-Tier Priority System section in the *Working with INCISIVE Support* section to understand each of the different support priorities.

Communication Method	Three-tier Priority Levels		
	Immediate	Urgent	Normal
Telephone	Immediately	Within 1 hour	Same day
Voice mail	Not recommended	Not recommended	Within 1 business day
Fax	Not recommended	Not recommended	Within 2 business days
Email	Not recommended	Not recommended	Within 2 business days
Instant Messaging	Not recommended	Not recommended	Within 1 business day

CrossCurrent Support Policy

We only support the current version of an INCISIVE product. If a problem exists with an earlier version of our software, we will ask customers to update to the latest version of the product to see if the problem remains in the current version of the product.

Automatic Updates

As we enhance or correct the software, we distribute product releases to customers using a web-updating feature built into our INCISIVE products. For critical updates, we notify customers by email, explaining the nature of the update and what actions, if any, our customers need to take. Each time the customer starts an INCISIVE product, the application will check update availability and proceed to download and update the application automatically. This process may take several minutes to complete; we apologize for this inconvenience, but we believe the benefit of not having to manage our applications outweighs this occasional inconvenience.

Remote Assistance

In order for us to provide meaningful support to your clinic, our Support Representatives must be able to connect to your workstations remotely. We can connect using our web conferencing or remote assistance tools. We are confident our remote access meets your organization's confidentiality and security requirements, as well as federal and state regulations governing the privacy and security of patient data.

Direct remote access offers the highest level of support to diagnosis, troubleshoot, and correct your issues while talking with a Support Representative. Direct remote access also provides the fastest possible response to such incidents. If direct remote access is not available, incident time can be significantly slower and take longer to resolve.

Your License and Support Agreement governs how remote access is set up between INCISIVE Support and your office locations. Remote access configuration should provide the following:

- A suitable Internet connection
- On our request and with your approval, we will access your system for error detection, analysis, replication, or correction. Our access will be subject to your prior approval in each instance.

① CrossCurrent will not be responsible for any failure to perform its obligations under its License and Support Agreement that results from the customer's refusal to provide us with access to their system.

On-site support services

On-site support service is not part of the regular Support Plan for INCISIVE products. However, on a case-by-case basis, the customer and CrossCurrent may agree to an on-site visit. Please refer to your Support Agreement for a definition of the conditions under which a site visit may occur and the fees associated with the visit. The visit cost estimates and payments will be governed by the Professional Services terms and conditions agreement.

Third-party software and support policies

We test INCISIVE products on selected Microsoft operating systems as listed in each product's recommended workstation configuration document. You can download these documents from our Support website. Customers can check the Microsoft Windows Life-Cycle website to determine when we will no longer be testing and supporting an end-of-life Microsoft operating system.

Windows Life-Cycle Policy

<http://www.microsoft.com/windows/lifecycle/default.msp>

Scope of support for client operating system software products

We provide the following support for client operating systems software:

- **Answering questions about how INCISIVE products work with operating system software.** INCISIVE Support Engineers are knowledgeable about how our products work with supported operating system software. However, if your question is related to the use of operating system software, we will ask you to call that particular company.
- **Isolating operating system software problems.** Is your problem related to the operating system software, INCISIVE software, or to another vendor's software? Because our software operates in a complex environment, the source of a problem is not always immediately evident. We will work with you to isolate issues, beginning with reproducing the problem. If your operating system software support services are provided by a third-party vendor, when necessary we will work with your supplier to isolate the problem.
- **Reporting SQL Defects.** Reproducing and submitting operating system software defects that directly relate to the use of INCISIVE software. We will submit defects

to an operating system software company that relate directly to the use of our products.

If a defect can be reproduced, that relates directly and only to INCISIVE products, we will contact Microsoft and either submit a defect report or accept and qualify an available patch/fix.

If a defect cannot be reproduced at your site or by us, but it recurs, we will contact Microsoft. If Microsoft has a fix or patch, we will qualify it. Otherwise, depending on the severity of the problem, we will work with you to develop a workaround.

If a problem is not reproducible at your site or by us and Microsoft has not heard of the problem and cannot recreate it, problem solving activity will cease until the problem recurs.

- **Informing customers of operating system software defects or releases that seriously affect use of INCISIVE software.** As an operating system software support services customer, we receive information regularly about the latest operating system patches and intermediate releases. We forward to you any information about the operating system that affects our software at your site.

If an available patch resolves a known critical defect affecting the use of INCISIVE software, we will attempt to qualify the patch with the current release and make it available to you.

- **Qualifying patches for operating system software defects that directly impacts use of INCISIVE software.** Whether we qualify an available operating system fix or patch depends on the circumstances. For example, if your production system is down and a patch might resolve the problem, we might recommend applying the patch with the understanding that it has not been qualified.

Remote Terminal Services

We do not have the testing capacity to test INCISIVE MD in remote terminal services environments like Microsoft Terminal Services or Citrix Presentation Server. However, we do have several customers successfully using INCISIVE MD in these environments. We urge customers who have these types of computing environments to install and test our software for their particular environment before deployment to users. Please contact INCISIVE Support for technical details regarding memory footprint, hard drive space requirements, and client software installation.

Microsoft SQL Support

Microsoft SQL is the standard database used with INCISIVE products. Each version of INCISIVE software is developed and tested with a particular version of Microsoft SQL. We will support the versions of Microsoft SQL certified for supported versions of INCISIVE products.

Since we host the INCISIVE software database servers, the scope of our support of Microsoft SQL in your computing environment is as follows:

- **Answering questions about using Microsoft SQL with INCISIVE products.** Many of our Support representatives are proficient in the Microsoft SQL database. However, we will direct you to contact Microsoft SQL Support Services to answer questions, provide defect information, or help resolve a problem with any Microsoft SQL Server you maintain.

- **Isolating Microsoft SQL problems.** Is your problem related to Microsoft SQL, our software, or another vendor's software? Because our software operates in a complex environment, the source of a problem is not always evident. INCISIVE Support works with you to isolate issues, beginning with reproducing the problem.
- **Reporting SQL Defects.** Reproducing and submitting Microsoft SQL defects that directly relate to the use of INCISIVE products. We will submit defects to Microsoft that relate directly to the use of our INCISIVE products.

If a defect that relates directly to the use of INCISIVE software can be reproduced, we will contact Microsoft Support and either submit a defect or qualify an available patch or fix.

If the defect cannot be reproduced at your site or by us, but it recurs, we will contact Microsoft Support. If Microsoft Support has a fix or patch, we will qualify it. Otherwise, depending on the severity of the problem, we will work with you to develop a workaround.

If a problem is not reproducible at your site or by us and Microsoft Support has not heard of the problem and cannot re-create it, problem solving activity will cease until the problem recurs.

We do not test and distribute Microsoft patches and other intermediate releases as they become available. Instead, upgrades and patches are rolled into the next scheduled server maintenance update. If a Microsoft upgrade or patch resolves a known critical defect affecting the use of INCISIVE software, we will qualify the release or patch with our software and make an emergency server software update.

The contents of your database belong solely to you, so any CrossCurrent approved changes to it will require prior written approval by a senior member of your clinic. We will work with you to ensure your database's structure and integrity.

Document Delivery to email or fax servers

INCISIVE products can send documents to be either faxed or emailed to a non-INCISIVE user. We have limited capability to troubleshoot issues with email or faxing. If you call with an email or faxing software issue, INCISIVE Support will refer you to your software or Internet Service Provider (ISP) vendors. INCISIVE Support will work as a member of troubleshooting team led by the customer or the software vendor.

Printer support

INCISIVE products should work on all standard office printers. However, we have only formally tested our products with Hewlett Packard laser printers.

As a software company, our support for printers is limited to determining the cause of a printing problem:

- If the problem is caused by our software, we will resolve the problem
- If the source of the problem is your network or printer, you are responsible for resolving the problem

Backup software support

INCISIVE products do not include external backup software, and we do not test the compatibility of our software with any vendor's backup software. Therefore, we do not

support backup software. If you call with a backup software issue, INCISIVE Support will refer you to your backup software vendor. INCISIVE Support will work as a member of troubleshooting team led by the customer or the software vendor.

Document or image management systems support

Although INCISIVE products can view images stored or linked within in the application, we do not support document or image management software to view these images.

Working with INCISIVE Support

Three-tier priority system
Before you contact INCISIVE Support...
Researching a customer issue with remote assistance
Submitting defects and enhancements

This chapter provides an overview of support procedures—how CrossCurrent INCISIVE Support representatives will work with you when you have support needs.

Three-tier priority system

Assign this priority...	With this impact...	To this type of problem...	And contact us this way...
Immediate	High – Critical	Financial data is inaccurately calculated or displayed, or software is unavailable.	Telephone
Urgent	Medium – Serious	Financial data needed to make a billing decision is not available. Major feature is not working or the speed of the software is unacceptably and perceptively slow. Major impact upon the productivity of surgeons.	Telephone or email
Normal	Low – Minor	Issue with acceptable short-term workaround	Telephone, fax, or email

To help manage your support needs, INCISIVE Support uses a case tracking system to log all reported issues, whether by reported by telephone, fax, or email.

Within this system, we assign three levels of priority to cases:

	Immediate	Critical business impact
	Urgent	Serious business impact
	Normal	Minor business impact

Please report Immediate and Urgent cases by telephone to speed response.

Before you contact INCISIVE Support...

Before you call us...

- If you have one, please contact other INCISIVE product users who may be able to answer many common questions
- Consult online help and these resources available on the Support websites as they may provide an immediate solution to your problem:
- Release notes
- User guides
- Installation checklists

When you call INCISIVE Support...

- Have following information ready:
- Your customer ID number
- Your name, your clinic's name, and your organization's name
- The Case Number previously assigned to or associated with this issue
- Your phone and fax numbers
- Product(s) and version number(s) being used
- Version numbers and types of operating systems being used
- Error message numbers and text
- Detailed description of the problem
- Description of the business impact of the problem; for priority definitions, see “Three-tier priority system” section. The Support representative can help you determine the severity level.
- If the problem is reproducible, the documented steps required to reproduce it
- Ensure you have Internet connectivity so that INCISIVE Support can initiate a remote assistance session with you

? If you do not know your Customer ID number, please ask the Support representative

Reporting a problem by fax or email

When reporting a problem by fax or email, please remember to include the name of your clinic, name of the contact person, and how to contact them. If it is straightforward to you, please attempt to describe the issue you are encountering in the fax or email.

Typical Support Case Workflow

When you reach INCISIVE Support, a Support representative will ask you some preliminary questions while logging the case.

Identifying the caller

The Support representative who answers your call will ask you for identifying information:

- Your name
- The name of the clinic and organization
- Your customer ID number (required for calls outside of regular business hours)
- The incident number (if the call is in reference to an open incident)

Log the incident

The Support representative will log your incident into our Customer Relationship Management system and will give you a case number.

① Write down your case number for future reference. If your issue is not resolved during this call, you can expedite subsequent calls by referring to this number.

Assigning a priority

Based on your input, the Support representative assigns your incident a priority level that we will use to prioritize our work.

Connecting with the right Support representative

Given the varied background of our Support representatives, the individual who answers your call may not be an expert in the area where you need help. In these cases, we may transfer to the appropriate representative to assist you.

Researching a customer issue with remote assistance

To help diagnose or repair a problem, the Support representative may request a remote assistance session. They will walk you through using our remote assistance tool.

Troubleshooting a problem

To diagnose your problem, the Support representative may ask you detailed information about your network, Internet connection, and security and application setting on the computer experiencing the issue for which you called.

This information helps the Support representative:

- Reproduce a software failure when the product isn't functioning according to the product documentation
- Confirm whether the issue is with our products or with a third-party product
- Begin correcting the problem

If the problem cannot be reproduced, the Support representative will attempt to identify a workaround until the problem can be reproduced or corrected.

If the troubleshooting process points to a problem with the hardware, operating systems, network, backup software, or any other software, you will be asked to contact the appropriate resources within your company or the appropriate third-party vendor. Further work by us at this point is subject to additional charges.

① If you request on-site support service, you may be subject to additional charges. See “On-site support services policy”.

When diagnosis reveals a defect...

If a new defect is identified during the troubleshooting process, it is logged, assigned a tracking number, and sent to the Product Development group. The Support representative will check for an existing workaround, fix, or patch and communicate this to you. If no solution is currently available, INCISIVE Support will attempt to identify a workaround to be used until the problem is resolved via a fix, patch, or new release.

If your problem is the result of a known defect, the Support representative will provide you with the current status of the defect. Your incident is logged in the tracking system (and noted as a duplicate).

Before you hang up...

To ensure that follow-up to your incident meets your expectations, review this checklist with the INCISIVE Support Engineer before you hang up.

Case checklist

- Review the severity level
- Review action items for the Support representative
- Review action items you've agreed to
- Confirm who is responsible for calling back and when
- Confirm the case number

Starting Remote Assistance



To start a remote assistance session you can do it from the INCISIVE Support website or within INCISIVE MD. From within INCISIVE MD, you simply need to click on the **Request Remote Assistance** life preserver icon. This icon is located in the top toolbar while on the INCISIVE MD Dashboard or on the bottom button toolbars when either planning or coding a surgery, or auditing a payment. For INCISIVE PM customers, you will need to start a remote assistance session from the Support website.

We currently use Citrix Corporation's GoToAssist as our remote assistance tool. The connection between your workstation and the Support representative is securely encrypted.

From INCISIVE Support Website

As the request of your Support representative, you can initiate a remote assistance session by going to the INCISIVE Support website and under the **Need help fast?** heading, enter your name, select the Support representative from the drop down list, and click **Submit**. It's that easy!

From the INCISIVE MD Dashboard

You can request a remote assistance session once you are logged into INCISIVE MD from the dashboard. Just click on the **Request Remote Assistance** life preserver icon located in the upper right corner of the INCISIVE MD dashboard next to the Log Out button (see picture on the next page) to initiate a remote assistance session with an INCISIVE Support representative.



While Planning or Coding a Surgery

You can now initiate a remote assistance session while planning and coding a surgery. You no longer need to either close your work and return to the INCISIVE MD dashboard or start a remote assistance session from the INCISIVE Support web site. To initiate a remote assistance session with an INCISIVE Support representative, click on the life preserver button in the lower left corner of the Pre-Op Planning or the Post-op Coding wizards' button bars.



While in the Audit Payment Wizard

As with planning and coding a surgery, you can request remote assistance while using the Audit Payment wizard by clicking on the life preserver button in the lower left corner of the Audit Payment wizard's button bar.



No Support Representative Available

If you initiate a remote assistance session while our support representatives are busy with other customers or not logged into GoToAssist, you will see a dialog pop-up with the message "No representative is available to take your request". If you are not already on the phone with a support representative, please contact INCISIVE Support to see if a support representative can work with you.

If the Support representative logs in while you are attempting to start the remote assistance session, please click Retry after the Support representative informs you that they are logged into the GoToAssist application.



Support Session Feedback

After completing a remote feedback session with one of our Support representatives, you have an opportunity to provide feedback to us and your Support representative on how well they did in helping you

with your problem. We strongly encourage you in providing this feedback to us. We review this feedback monthly with CrossCurrent executive management.

Submitting defects and enhancements

To submit a defect or enhancement request, you can:

- Call INCISIVE Support
- Use the Contact Us web form from the Support website

How we handle defects and enhancement requests

When we receive your defect report or enhancement request, we log it and assign a tracking number for future reference. If you report a defect or enhancement by phone, we enter the defect, assign a tracking number, and create a case in our Customer Relationship Management system. If you make the request using the Product Feedback form, you will receive an email response.

Escalating incidents, defects, or enhancements

If you feel INCISIVE Support is not providing the level of attention you believe is warranted for an incident or a logged defect or enhancement, you can request that it be escalated.

When requesting escalation, refer to the case number in all communication. When you contact us, ask a Support representative to connect you with the INCISIVE Support Manager. If the manager is unavailable, he or she will respond as soon as possible to discuss the situation and work with you to create a plan to resolve the issue.

If the INCISIVE Support Manager is unable to resolve the problem, or is not providing the level of attention you believe is warranted, escalation may continue to the Chief Executive Officer.



CrossCurrent

5331 SW Macadam Ave Ste 216
Portland OR 97239-3873

Voice | (503) 248-2290
Fax | (866) 899-2746

www.incisivemd.com

PN 4501
Release |
9 Sep 2011