CureMD™

Practice without boundaries

Support Policies and Escalation Procedures

ATTACHMENT B - GUILFORD COUNTY CONTRACT NO. 113348-03/16-271
CAROLINAS IT, INC. (PROVIDER)

Confidentiality and Proprietary Rights

Trademarks

Purpose of this Document

This document provides important information on the Support Policies and Escalation Procedures implemented by CureMD to ensure seamless application availability and resolve any issues that may arise.

ATTACHMENT B - GUILFORD COUNTY CONTRACT NO. 113348-03/16-271
CAROLINAS IT, INC. (PROVIDER)

Introduction

CureMD believes that having your business is both a privilege and a responsibility. We hope to maintain that business by providing you with solutions to your information technology problems. We also recognize that in order to enable you to concentrate on your core business issues, it is crucial that we provide world class information technology services that complement our healthcare information system solutions.

The intent of software support is to provide you with the quality software support and services you need. Our vision is to achieve a level of support excellence that exceeds your expectations and differentiates CureMD in the marketplace by providing:

- Rapid response to your requests
- Fast relief to high impact problems
- Timely problem resolution
- High quality fixes and information
- Up-to-date service and installation information.

We are committed to achieving the highest level of customer satisfaction in the industry, with quality focused programs designed to provide services that enhance and maximize the use of CureMD products. As your solutions partner, we are dedicated to enabling your success.

The CureMD Advantage

When you buy a CureMD solution, you become part of an exclusive club where all members are cherished and valued for their relationship with us. We ensure our eager support services continue to make you feel pampered and help you get the most of your software solution. To achieve this, a dedicated Account Manager and a Service Delivery Manager is assigned solely to your account. These individuals serve as your advocates here at CureMD and ensure that all your queries are addressed with the utmost urgency. The Account Manager and the Service Delivery Manager both will be assigned to you prior to your *Go-Live* date and an introductory meeting will be held to introduce them to your team.

Our Experience

CureMD is the leading provider of innovative health information management solutions that transform the administrative and clinical operations of healthcare organizations of all sizes. We have been successfully supporting thousands of doctors and their administrative staff for over 13 years. Our 100% customer retention rate speaks volumes of our support services. We utilize industry best practices and advanced support tools to help provide our clients the quality of support they expect.

Support Infrastructure

CureMD's software support organization is a global network of centers with expertise across our broad product portfolio. The organization is made up of teams of individuals that work together to provide you with the responsive software support that you require. Our worldwide centers are structured to provide you with local language access in most major countries and with the skills to help you identify the source of your problem amongst the products for which you have purchased support. For complex problems, we have specialized, skilled product teams with access to the experts in our Research and Development Centre, as required. Therefore, you have access to the right level of CureMD expertise when you need it -- no matter where they are located.

CureMD's support engineers are highly skilled, motivated, energetic, and eager to solve your software problems or answer your questions. Our goal is to ensure your satisfaction each time you need to call on us for support by:

- responding to your calls within targeted guidelines
- providing ongoing communication regarding your problem status through problem resolution
- taking ownership of your call for support
- providing a defined escalation process when management assistance is needed
- maintaining our commitment to continuous improvement of our service processes

Support @ Your Doorstep

Included in the acquisition of CureMD's Custom Healthcare Software is an enhanced level of support named "Support @ Your Doorstep". It is designed to provide comprehensive, high quality remote technical support to your Information Systems (IS) organization. Remote technical support allows you to obtain assistance from CureMD for product-specific, task-oriented questions regarding the operation of your CureMD software products. Our support teams utilize remote access tools including Citrix ® GoToMeeting and Microsoft ® WebEx to connect directly to any computer on-site and address specific issues.

Support Methodology

In order to understand and resolve customer software support service in the most expedient way possible it is important that our customers follow these steps before contacting a software support center. They need to gather information about the problem and have it on hand when discussing the situation with the software specialist. The following steps are an example of what is required:

Define the Problem

Being able to articulate the problem and symptoms before contacting software support will expedite the problem solving process. It is very important that our customers are as specific as possible in explaining a problem or question to our software specialists. Our specialists want to be sure that they provide you with exactly the right solution so, the better they understand your specific problem scenario, the better they are able to resolve it.

Gather Background Information

To effectively and efficiently solve a problem, the software specialist needs to have all of the relevant information about the problem. Being able to answer the following questions will help us in our efforts in resolving your software problem:

- What module(s) of the software were running when the problem occurred?
- Has the problem happened before, or is this an isolated problem?
- What steps led to the failure?
- Can the problem be recreated? If so, what steps are required?
- Have any changes been made to the system? (hardware or software)
- Were any messages or other diagnostic information produced? If yes, what were they?
- It is often helpful to have a printout of the message number(s) of any messages received when you place the call for support.

Gather Relevant Diagnostic Information

It is often necessary that our software support specialists analyze specific diagnostic information, such as server logs, traces, etc., in order to resolve your problem. Gathering this information is often the most critical step in resolving customer problem. Module specific diagnostic documentation can be very helpful in identifying what information is typically required to resolve problems.

Determine Business Impact

Customers are required to assign a severity level to the problem when they report it. A description of the severity levels is in the following table.

Severity 1 (Critical)	**Severity 2 (High)**	**Severity 3 (Medium)**	**Severity 4 (Low)**
Business and financial exposure			
The application failure creates a serious business and financial exposure.	The application failure creates a serious business and financial exposure.	The application failure creates a low business and financial exposure.	The application failure creates a minimal business and financial exposure.
Work Outage			
The application failure causes the Client to be unable to work or perform some significant portion of their job.	The application failure causes the Client to be unable to work or perform some significant portion of their job.	The application failure causes the Client to be unable to perform *some small* portion of their job, but they are still able to complete most other tasks. May also include questions and requests for information.	The application failure causes the Client to be unable to perform a *minor* portion of their job, but they are still able to complete most other tasks.
Number of Clients Affected			
The application failure affects a *large* number of Clients.	The application failure affects a *large* number of Clients.	The application failure affects a *small* number of Clients.	The application failure may only affect one or two Clients.
Workaround *[This bullet carries the heaviest weighting of the characteristics for Severity 1 and 2.]*			
There is no acceptable workaround to the problem (i.e., the job cannot be performed in any other way).	There is an acceptable and implemented workaround to the problem (i.e., the job can be performed in some other way).	There may or may not be an acceptable workaround to the problem.	There is likely an acceptable workaround to the problem.
Response Time			
Within two hour.	Within four hours.	Within eight hours or by next business day (EST).	Within eight hours or by next business day (EST).
Resolution Time			
The maximum acceptable resolution time is	The maximum acceptable resolution time is	The maximum acceptable resolution time is	The maximum acceptable resolution time is

Severity 1 (Critical)	Severity 2 (High)	Severity 3 (Medium)	Severity 4 (Low)
48 continuous hours, after initial response time.	seven business days.	30 business days.	90 calendar days.

When speaking with a software support specialist, our customers are encouraged to mention the following items if they apply to their unique situation:

- you are under business deadline pressure
- your availability (i.e. when you will be able to work with CureMD Software Support)
- you can be reached at more than one phone number
- you can designate a knowledgeable alternate contact with whom we can speak
- you have other open problems with CureMD regarding this service request
- you have researched this situation prior to calling CureMD and have detailed information or documentation to provide for the problem.

Support Request Process

Call Handling

Customers may submit request for assistance by using Web problem submission tool(s) or by contacting CureMD directly by telephone, fax or email. These requests are logged into the CureMD Issue Tracking system.

Once logged, a unique Case ID is created. Customers are required to make note of this Case ID and use it in any future communication on this issue with the support center. Once registered each support case is routed to a resolution team for handling. Customers may be transferred directly to the resolution team or your issue will be placed in a queue for call back. In either case, the next person they speak with will be a specialist in the appropriate resolution team.

At the resolution team level customer call is researched, resolved, or escalated as appropriate. Due to the level of specialization required to maintain superior technical expertise at the team level, it is sometimes necessary to involve more than one support team in resolving a particular software problem. This is easily handled, as our support teams are all networked together and work as one to resolve whatever problems or issues arise.

In order to investigate the issue, CureMD may need to access information on your system relative to the failure, or may need to recreate the failure to get additional information.

Code Defect Handling

If CureMD determines that a software defect has been identified a Change Control Board Report (CCBR) will be created which describes the problem in detail, along with any necessary diagnostic documentation that our customers provide. Because of the complexities of the software, CCBRs will often take several days, to debug and to write, test, package and distribute a fix. For high impact problems, CureMD Software Support will make every effort to develop a bypass or workaround that can be used until the CCBR has been resolved. Code fixes for CureMD products may be distributed via software subscriptions, service packages or in a future release of the product.

Escalation Procedures

We believe CureMD Support is "Best of Breed." If at any point in our service process, if our customers feel we are not meeting our commitments, they may call our attention to this problem by asking to speak with your Project Manager or by calling your Account Manager or Service Delivery Manager. Escalations to a CureMD manager will receive prompt attention and management focus. The Manager will work with our technical staff to ensure your request is handled appropriately.

Practice without Boundaries

CureMD is the leading provider of Cloud based EHR, Practice Management and Medical Billing services to transform the administrative and clinical operations of healthcare organizations of all sizes. Our award winning solutions simplify decision making, streamline operations and ensure compliance with industry standards and best practices - ultimately saving time and effort to maximize value and returns.

CureMD Healthcare
120 Broadway, 35th Floor
New York, NY 10271
Phone: +1 (866) 643 836
www.curemd.com

CureMD™

Practice without boundaries

Implementation Life Cycle

Implementation Methodology and Plan

Phased Approach

CureMD has built a tremendous track record over the last 18 years of very successful implementations. We understand healthcare. We understand IT. We understand that every healthcare organization is unique. So we take the time to understand your needs and make sure to meet them.

To ensure the success of our implementations, we have developed a proven methodology that has been used in thousands of successful implementations nationwide. Our methodology, designed with a balance between structure and flexibility, enables us to provide a fast, efficient, economical implementation of CureMD software and solutions every time.

CureMD is structured for scalability, implementation ease, and rapid deployment and is continuously enhanced with these goals in mind. Our site-by-site phased implementation approach allows for a gradual evolution of information systems in your organization as your expand, add more services or innovate new ways or working.

Benefits

Care delivery organizations demand minimal business disruption and predictable implementation costs. Many of our clients have replaced existing legacy systems with CureMD and our comprehensive paper to electronic system conversion procedures cover a variety of workflow and operational systems. As a result, you benefit from our experience and replacing your existing paper based system can be done efficiently and cost effectively.

The winning formula that ensures your success is the combination of CureMD's implementation methodology, aggressive project management, enterprise class system and technological expertise, world class education and superior training methods—all packaged to get you up and running quickly to enable a quick return on your system's investment.

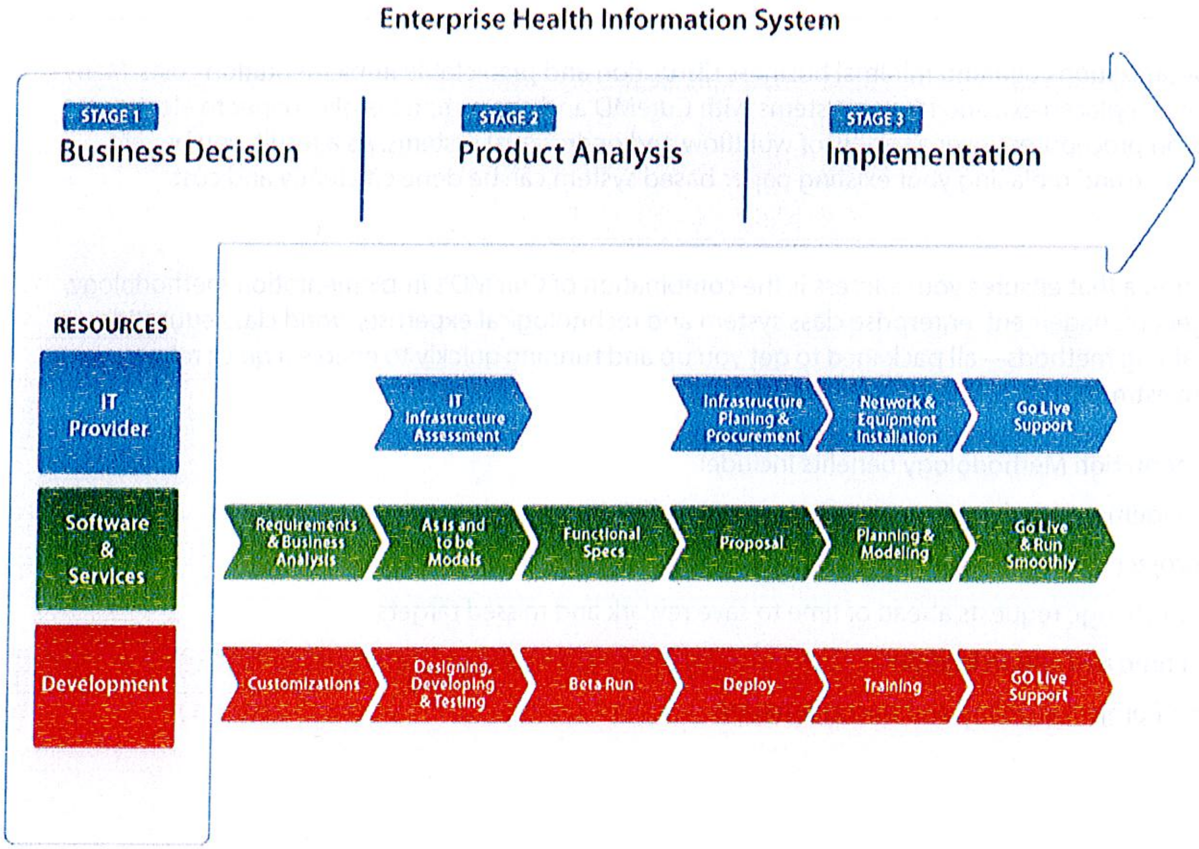
CureMD Implementation Methodology benefits include:

- Secured management involvement, governance, and oversight
- Controlled project costs and schedules-solutions
- Implementing change requests ahead of time to save rework and missed targets
- Delivered on time and within budget
- High degree of project visibility and documentation

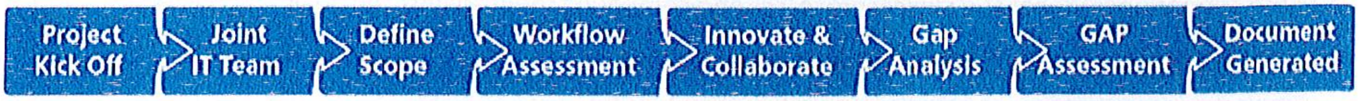
Phased Implementation Methodology

CureMD implementation service includes assessment, gap resolution and readiness, application configuration, installation, training and support. These phases are designed to provide our client with a seamless transition from an existing electronic or paper-based system to the CureMD system while ensuring that all aspects of the client organization´s operations are fully supported and accounted for.

With CureMD, our customers acquire seasoned on-site staff comprising of highly competent application analysts, IT engineers, project managers and program architects to deliver synchronized energies to support a rapidly updated product backed by outstanding L1, L2 & L3 support to constantly and effectively meet changing user and organizational requirements.



Assessment Phase (Current State Review)



The timeline begins with an assessment phase, key objectives of which are to understand the current situation and develop a plan to implement the CureMD solution most efficiently within the client organization.

The Assessment phase is preceded by the project kick-off work-session that includes application demonstrations, completion and review of requirements and configuration questionnaires as well as delivery of client documentation. The Project Kick-off will provide your organization with the opportunity to not only introduce the CureMD Project Team to your organization, but also to define and structure your organization's Project Team. Detailed process documents covering all aspects of the implementation are provided; these include client responsibilities as well as the best practice approaches to project implementation that CureMD has evolved after years of success implementations.

The information obtained during this phase ensures CureMD solution is configured specifically for customer organization including such information as administrative and clinical work flows, treatment plan design, user-definable tables and lists, configurable modules, reporting requirements, applicable policies and procedures, information security, government and accreditation regulations, etc. Integration, interfacing and data migration requirements are also defined during the assessment process.

After both project teams are introduced, a critical step in the process is building a joint team to conduct a detailed organizational assessment, collaborate to preserve existing efficient workflows and functionalities, and innovate to introduce practice process reengineering; eliminating redundancies to ensure organizational success. The team, led by a CureMD senior project manager will include representation from all pertinent departments and stakeholders such as clinician and administrative users, management representatives, and internal IT support team.

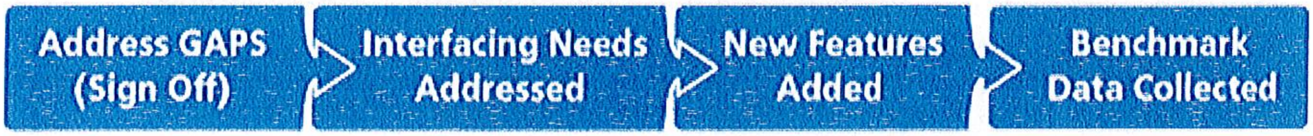
The assessment executed by the team will define the scope of the project in terms of the functions and departments to be supported. A detailed workflow analysis of the scoped functions is also performed to understand gaps and redundancies.

A comprehensive gap analysis carried out by CureMD will include (i) review of current operational workflow processes, (ii) existing information systems, functionality and use, (iii) existing interfaces, (iv) reporting tools, (v) manual processes, (vi) forms and documents, (vii) organizational structure, (viii) policies and procedures and (ix) training and support.

Results of our gap analysis will determine where organization currently stands (as-is) and what needs to be done (to-be) to accomplish the goals and objectives set out at the beginning of the implementation. By analyzing the current operational and clinical processes and comparing them against the goals and objectives, CureMD will identify areas requiring process improvement to ensure compliance with best practices as appropriate to the organization.

In this phase, the team also develops the implementation plan with implementation milestones and deliverables for a clear roadmap and role clarity for team partners.

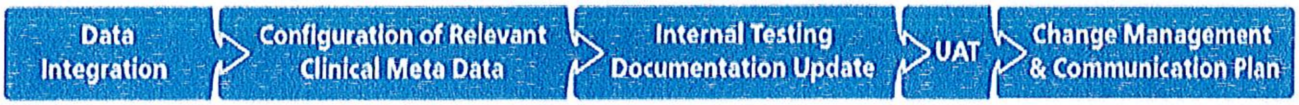
Gap Resolution & Readiness Phase



As the first phase yields the specific client requirements, the gaps identified and deemed essential therein are closed. These requirements are used by CureMD implementation team to configure the CureMD solution as equired by the client organization. In addition, readiness activities are undertaken. This includes addressing interface requirements as identified in the scope, such as developing and testing HL7 messaging brokers or other interfacing solutions for data exchange. Simultaneously, pre-implementation benchmark data for comparison is collected to provide useful inputs in determining the impact the solution has had in improving efficiency, quality, and financial returns.

GAP resolution phase also includes configuration, data entry and may include data migration identified during the Assessment phase.

Application Configuration Phase (User Acceptance Testing - UAT)


Data Integration
Configuration of Relevant Clinical Meta Data
Internal Testing Documentation Update
UAT
Change Management & Communication Plan

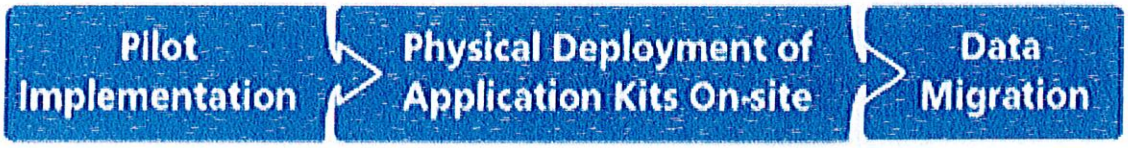
This phase begins with validating the integrity of data onto the new solution. The relevant functional data sets are mapped between the legacy or paper based system to assist in transferring existing information across to the new database. Relevant clinical and other information dealing with forms, templates, alerts, drug and laboratory order sets, specific reference terminologies used with the customer organization, user profile mapping, and other requirements are configured into the system. The solution undergoes rigorous internal testing to determine the correctness of the data migration and configuration. End-user functional testing is also executed in this phase to confirm the clinical correctness of migrated information. This phase also involves detailed documentation of configured features as well as training templates for support. The implementation team also develops a change management plan addressing which users and departments to target, the most effective mode of communication and how to overcome change resistance.

User Acceptance Testing (UAT) includes four critical functions in the project cycle: training, user proficiency, process definition and finalization of specifications including configuration, customization and data migration. The UAT process starts with a series of formal on-site user training sessions followed by hands-on system use, allowing customer organizations to practice using the system, conduct additional internal training sessions and begin creating task level procedural documentation. Additionally, this will provide users with more in-depth knowledge of CureMD functionality, which may lead to additional configuration, data migration or manual data entry.

The UAT period will culminate with CureMD's finalization of quality assurance testing and delivery of configuration updates in preparation for production rollout. CureMD offers additional training, process analysis/re-engineering as well as Client-side project management services as needed throughout the UAT progress period.

Implementing new EHR also means a change in culture and employee attitude and behavior. It is, therefore, essential to have a change management process in place to ensure that staff is cooperative and embraces the changes that must take place to ensure a successful implementation. A change management plan for an Enterprise EHR implementation will include a methodology incorporating (i) communication; (ii) explanation of the business reasons for change; (iii) the cost and risks of not implementing the EHR; (iv) positive impact the EHR will have on the organization; (v) goals and objectives; (vi) involvement of staff at all levels; (vii) training on workflows and system; (viii) policies and procedures and (ix) celebration of the success of the implementation as well as recognition of accomplishments.

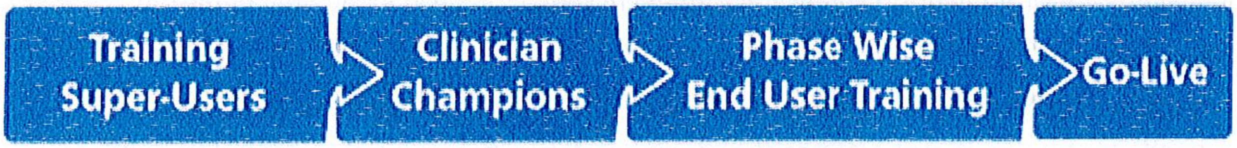
Installation Phase (Production Roll Out)


Pilot Implementation
Physical Deployment of Application Kits On-site
Data Migration

In this phase, a master production rollout plan is developed detailing staff communication, training schedule and scheduling of CureMD on-site production support resources. Also the network, hardware and application infrastructure is physically installed on-site and detailed data migration process is carried out. Prior to this phase, CureMD works with the customer to evaluate which department should be the first to launch the new system.

The plan also includes identification of power users who serve as client functional experts, as part of the "Train the Trainer" model, as well as individuals who will require specialized or more focused training. Additionally, an internal communication plan is established to notify users of the transition to CureMD and of any expected impact on staff responsibilities. Finally, production rollout planning includes the scheduling of CureMD trainers and production support specialists to assist in the execution of the rollout plan and provide on-site support during the initial week(s) of the production rollout.

Training Phase

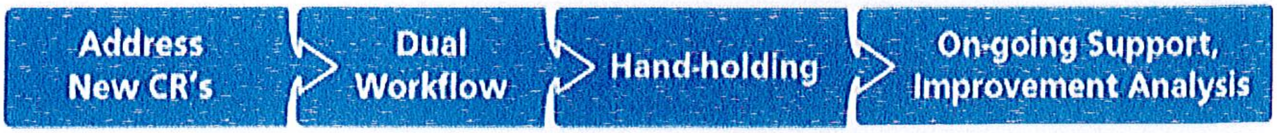

Training Super-Users
Clinician Champions
Phase Wise End User Training
Go-Live

Training includes super-user training which would then help in training other users in phases. Carefully identifying a clinician champion at this juncture promotes the physician acceptance within the doctor network. Based on user comfort and stability of the application, a go-live date is set.

System is implemented in the production environment with partial functionalities, on site staff is made available to collaborate and help resolve any unforeseen issues including transaction processing support if required.

As users become proficient with the system, additional modules are introduced leading to full product implementation.

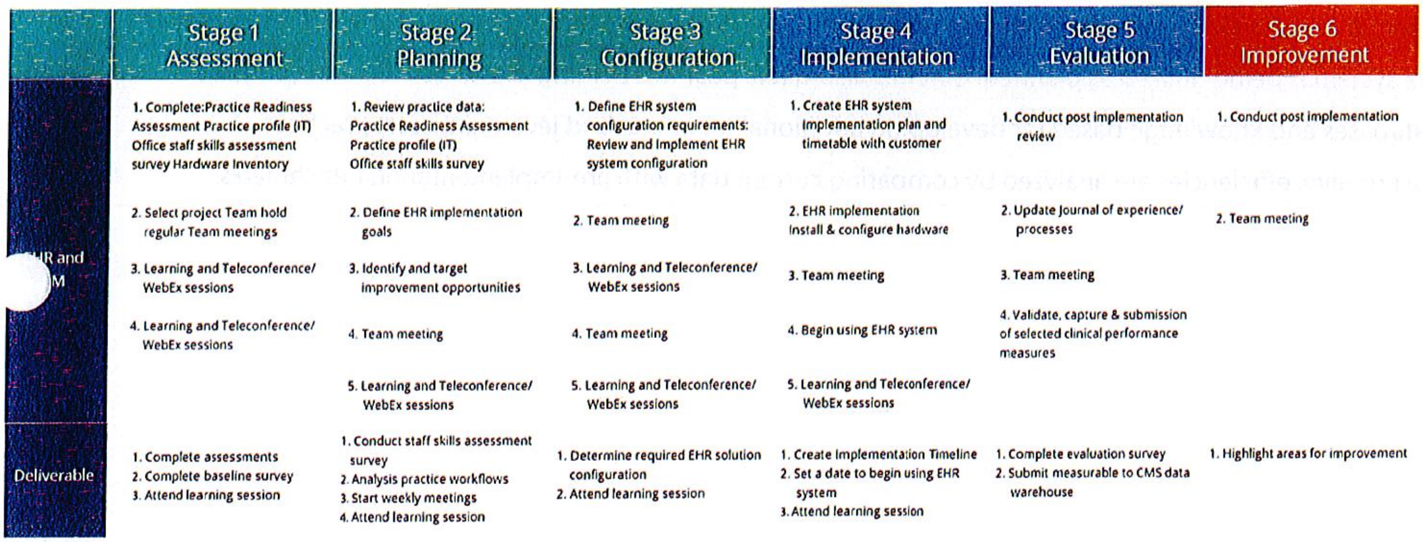
Comprehensive Support Phase


Address New CR's
Dual Workflow
Hand-holding
On-going Support, Improvement Analysis

This phase involves addressing any new change requests due to unforeseen configurations. The department maintains dual work-flows in parallel for a period of time to take care of any contingencies as well as to gain end-user confidence in the system. A period of handholding by the joint support team is determined which later moves into an on-going support phase. There are various types of Support rendered but the critical needs are education support, end user support, and technical support.

After go-live, CureMD conducts follow-up with the end-users to ensure that the issues, if any, are resolved and the system is being utilized as planned. CureMD also offers post-live training as well as a Clinical content databases and knowledge based for developing additional templates and leveraging best practices.

Post go-live, efficiencies are analyzed by comparing current data with pre-implementation benchmarks.



	Stage 1 Assessment	Stage 2 Planning	Stage 3 Configuration	Stage 4 Implementation	Stage 5 Evaluation	Stage 6 Improvement
HR and M	1. Complete:Practice Readiness Assessment Practice profile (IT) Office staff skills assessment survey Hardware Inventory	1. Review practice data: Practice Readiness Assessment Practice profile (IT) Office staff skills survey	1. Define EHR system configuration requirements: Review and Implement EHR system configuration	1. Create EHR system Implementation plan and timetable with customer	1. Conduct post implementation review	1. Conduct post implementation
	2. Select project Team hold regular Team meetings	2. Define EHR implementation goals	2. Team meeting	2. EHR implementation Install & configure hardware	2. Update Journal of experience/ processes	2. Team meeting
	3. Learning and Teleconference/ WebEx sessions	3. Identify and target improvement opportunities	3. Learning and Teleconference/ WebEx sessions	3. Team meeting	3. Team meeting	
	4. Learning and Teleconference/ WebEx sessions	4. Team meeting	4. Team meeting	4. Begin using EHR system	4. Validate, capture & submission of selected clinical performance measures	
		5. Learning and Teleconference/ WebEx sessions	5. Learning and Teleconference/ WebEx sessions	5. Learning and Teleconference/ WebEx sessions		
Deliverable	1. Complete assessments 2. Complete baseline survey 3. Attend learning session	1. Conduct staff skills assessment survey 2. Analysis practice workflows 3. Start weekly meetings 4. Attend learning session	1. Determine required EHR solution configuration 2. Attend learning session	1. Create Implementation Timeline 2. Set a date to begin using EHR system 3. Attend learning session	1. Complete evaluation survey 2. Submit measurable to CMS data warehouse	1. Highlight areas for improvement

Implementation Stage Timelines

	Tasks Recommended for successful movement along the EHR Implementation Roadmap	Milestone Checklist To demonstrate measurable movement along theEHR Implementation Roadmap	Tools and Services
ASSESSMENT	>> Complete HIT readiness >> Assess current workflow (identify pain points) >> Begin or continue regular staff meetings (at least monthly) >> Assign physician champion >> Organize an EHR implementation team >> Assign an individual (EHR team leader) or team to lead practice change Commit to: >> Full provider engagement to enter data >> Workflow changes necessary to maximize results	Date Milestone (4 Days) >> HIT readiness assessment/ enrollment form completed >> Readiness/next steps reviewed >> Physician champion assigned >> Team leader assigned for practice changes >> Current workflow processes assessed >> Proposed implementation target date	>> List of success factors >> Barriers and solutions worksheet >> Complete assessment >> Facilitate staff discussions >> Conduct workflow analysis
PLANNING	>> List clinic goals and priorities (include functions and specific provider needs) >> Translate identified EHR goals into EHR system functions and features >> Identify staff at lower levels of readiness, address their concerns >> Develop a timeline and project plan >> Gain support from team members and staff, prepare for change management	Date Milestone (5 Days) Identify goals, priorities and any staff concerns EHR goals and associated system functions are listed Implementation plan developed, includes such items as: Target implementation schedule/timeline Measurable EHR goals	>> Implementation plans and timelines >> Key features list >> Example goals >> Peer interaction >> Facilitate staff meetings
CONFIGURATION	>> Schedule structured sessions >> Identify configuration requirements for Quality Reporting, Specialty Customization and User Preferences >> Continue workflow assessment and changes >> Identify configuration requirements hardware, office wiring, and necessary network support for all services and products not included in EHR	Date Milestone (6 Days) EHR configuration identified Specialty and user specific templates and workflows implemented	>> Workflow and business process configuration tools >> Compliance worksheets >> User and Specialty based Configuration templates
EVALUATION	>> Assign data manager/administrator >> Assure data conversion and testing completed >> Create data recovery and security plans >> Assure interfaces completed and tested for: >> Practice Management System Laboratory >> Other (Equipment, Radiology, Referrals) >> Determine a "go-live" date >> Train staff >> Celebrate success and address problems	Date Milestone (10 Days) Data manager assigned Data conversion and testing completed Interfaces tested and working properly "Go-live" completed and celebrated CureMD will be the primary driver of this stage, but the customer should be thoroughly engaged in all aspects of implementation.	>> Guidelines for reporting and quality indicators >> Assistance trouble shooting reports
IMPROVEMENT	>> Commit to continuous review of clinical and administrative processes >> Systematically increase the number of EHR functions used by providers and staff. >> Identify and target additional care management and process improvement opportunities >> Use EHR to optimize practice of evidence-based medicine >> Participate in user groups >> Continue creating quality reports	Date Milestone (Ongoing) Reanalyze clinical and administrative processes Functions used increases monthly Review performance reports Identify quality improvement opportunities Redesign work processes to use EHR clinical decision support tools with each patient encounter	>> Best practice solutions to improve performance data >> New workflow analysis

Practice without Boundaries

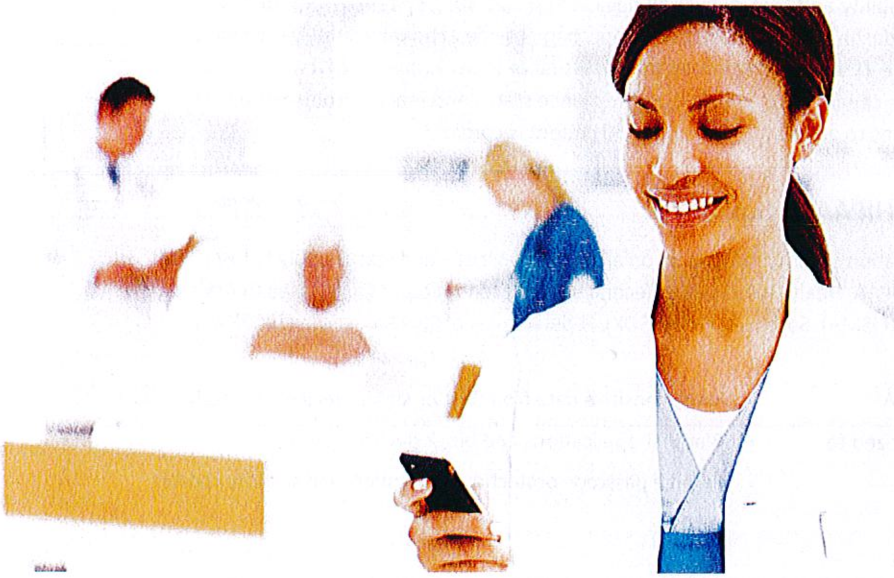
CureMD is the leading provider of Cloud based EHR, Practice Management and Medical Billing services to transform the administrative and clinical operations of healthcare organizations of all sizes. Our award winning solutions simplify decision making, streamline operations and ensure compliance with industry standards and best practices – ultimately saving time and effort to maximize value and returns.

CureMD Healthcare
120 Broadway, 35th Floor
New York, NY 10271
Phone: +1 (866) 643 836
www.curemd.com

MaaS360®
by Fiberlink, an IBM company

TruSaaS™

MaaS360® for Healthcare



MaaS360 in Action: Millions in HIPAA Fines Wiped Clean

A physician relies on an iPhone to access medical reference libraries, patient records and lab results—in addition to calendar scheduling, voice and text messaging. On a speaking engagement abroad, the iPhone is stolen—on a bistro table one minute, gone the next.

Without hesitation, the physician calls the hospital where he is on staff and directs the IT department, equipped with MaaS360, to wipe all information from the device, which is done by the IT department remotely in a matter of minutes.

Protect Patient Information

HIPAA

Healthcare-Specific Challenges

Physicians and healthcare workers increasingly depend on their own mobile devices to access medical and patient data at the point of care. At the same time, healthcare organizations face greater liability and fines if found out of compliance with HIPAA under a new audit program mandated by the 2009 HITECH Act, where the maximum penalty was increased to $1.5 million.

While mobile technology improves the quality and cost of patient care, it increases IT workloads and the potential for information security and HIPAA compliance risks. IT is expected to manage all of these risks while improving the productivity of your healthcare colleagues and keeping them happy by allowing them to use their own mobile devices.

MaaS360 Healthcare Solution

MaaS360 enables organizations to secure electronic protected healthcare information (EPHI) on all mobile devices connecting to their network, comply with HIPAA and other regulations, and reduce the IT workload and cost of managing mobile devices.

Using MaaS360, Mobile Device Management (MDM), Mobile Application Management (MAM), and document and expense management can be easily and instantly integrated into broader enterprise programs for IT governance, data security and regulatory compliance.

Key Benefits

- Gain 360° visibility and control of all mobile devices, apps, documents and files
- Automate password, encryption and policy enforcement
- Ensure anytime, anywhere device and data security with immediate remote action on nonconforming devices
- No infrastructure changes required
- Rapid implementation
- Low implementation costs and no-fuss maintenance
- Expense management to control costs and overages

Key Features

- Supports today's mobile devices from a single console, including iPhone, iPad, Android, Windows Phone, BlackBerry and Kindle Fire
- Instant device enrollment via SMS, email or URL over-the-air (OTA)
- Pushed policies, encryption and security safeguards
- Contextual, event-based policy, security and compliance rules engine and automation
- Enforce usage policies specific to physicians, healthcare workers and staff
- Remote locate, lock and wipe (full and selective)
- Blacklisting, whitelisting and requiring apps
- Customized app catalog
- Support for custom apps
- Control document distribution
- Real-time reporting and analytics

MaaS360®
by Fiberlink, an IBM company

MaaS360 for Healthcare

Control All Devices

MaaS360 gives healthcare organizations coordinated visibility and control over all devices and operating systems, from Apple iOS to Android, Windows Phone and BlackBerry. Integrated dashboards, analytics, and reporting provide actionable intelligence about their entire mobile environment through a single console. IT administrators can quickly visualize the distribution of devices, apps and documents across platforms, approval status, device capabilities, ownership, compliance status and more to control the risks of physicians and healthcare workers using mobile devices to access medical apps and patient records.

Improve Mobile Information Security and HIPAA Compliance

MaaS360 provides the ability to know and control information security safeguards on all mobile devices – and react rapidly to lost or stolen devices to ensure regulatory compliance with HIPAA, Health Information Technology for Economic and Clinical Health Act (HITECH), Federal Information Security Management Act (FISMA), Sarbanes-Oxley (SOX), Federal Rules of Civil Procedure (FRCP) and other statutes. IT departments can:

- Push policies and Wi-Fi, email and VPN profiles OTA
- Quarantine new devices automatically until authorized to access your network
- Wipe sensitive data from lost or stolen devices remotely
- Blacklist applications and block device access
- Enforce passcode protection, encryption, and security updates

Control Mobile Applications

MaaS360 application management allows healthcare organizations to easily manage and secure the applications that are critical to your users (e.g. Electronic Health Records (EHR), Computerized Physician Order Entry (CPOE), Diagnostic Imaging, Patient Vitals Monitoring, Point of Care, etc.). An on-device application provides users with a catalog of authorized private and public apps. Users can view the apps made available to them, install apps, and be alerted to updates. IT and other departments can manage the master app catalog and per-user authorization. Application lifecycle management provides real-time software inventory reports, app distribution and installation tracking, update publishing, provisioning profile management, and app security and compliance management.

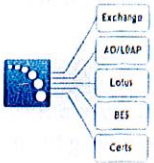
Reduce IT Workload and Costs

With MaaS360's true SaaS model, there are no servers to install, no complex configurations or infrastructure changes, and no investment in expensive business software. Built on a secure, multi-tenant cloud architecture, Maas360 enables instant enterprise mobility management in just minutes with effortless scalability, whether from ten to tens of thousands users, and seamless integration into existing enterprise systems. Additionally, MaaS360 eliminates the strain and expense that rapidly changing mobile devices and applications used by physicians and healthcare workers can have on IT organizations by automatically incorporating the continuous stream of platform updates.

Why MaaS360

Proven approach to cloud-based mobility management

Powerful management & security to address the full mobility lifecycle



Seamlessly integrates with all of your existing infrastructure

Simple & fast with an exceptional customer experience

All brands and their products, featured or referred to within this document, are trademarks or registered trademarks of their respective holders and should be noted as such.

For More Information

To learn more about our technology and services contact Carolinas IT
Phone 919.573.4083 | Email info@carolinasit.com

CureMD™
Practice without boundaries

Production System Architecture

Copyright Notice

Confidentiality and Proprietary Rights

CureMD™
Practice without boundaries

Contents

CureMD™
Practice without boundaries

1. Purpose

This document provides an overview of infrastructure and scalability architecture for CureMD solution to achieve:

Option 1: Single Site Disaster Recovery

- 99.8% uptime, excluding scheduled maintenance.
- Unlimited Scalability.

Option 2: Offsite Disaster Recovery

- 99.9% uptime, excluding scheduled maintenance.
- Unlimited Scalability.

2. System Architecture

CureMD solution is available with both options.

Option 1 offer a combination of high availability equipment and fault tolerant infrastructure utilizing redundant load balancers, web and data base servers and network are employed to deliver business continuity at 99.8%.

Option 2 ensures 0.1 % or 9 hours of additional availability though redundant infrastructure at an extended site where data is replicated through IP SAN across the two sites in near real time. This option requires almost double the cost.

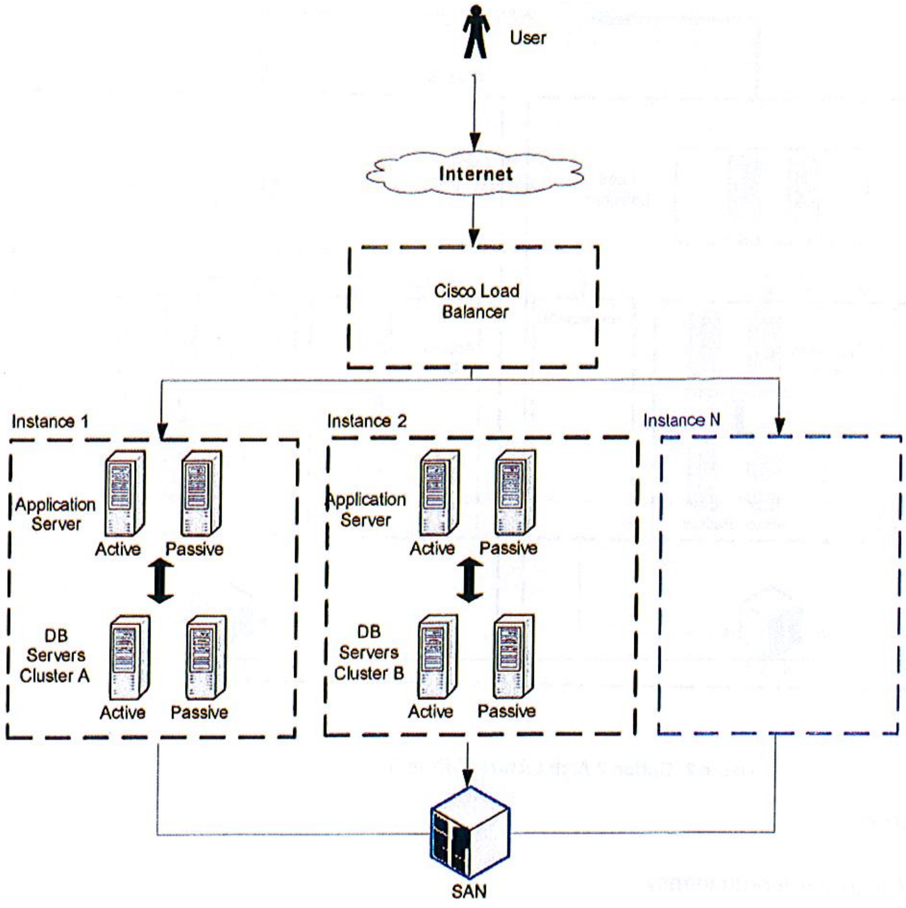


Figure 1: Option 1 Architecture (Single Site)

Single Site Infrastructure:

- Load balancer routing users to their receptive instance capable of multiple instance handling (Scalability)
- Application fail over cluster
- DB Server failover cluster
- SAN fail over Cluster
- Fault is contained to the failing component and does not propagate to other components.
- "Scaling out" technique is used to increase capacity when required. As the number of providers/practices increase, additional instances will be added to distribute load.

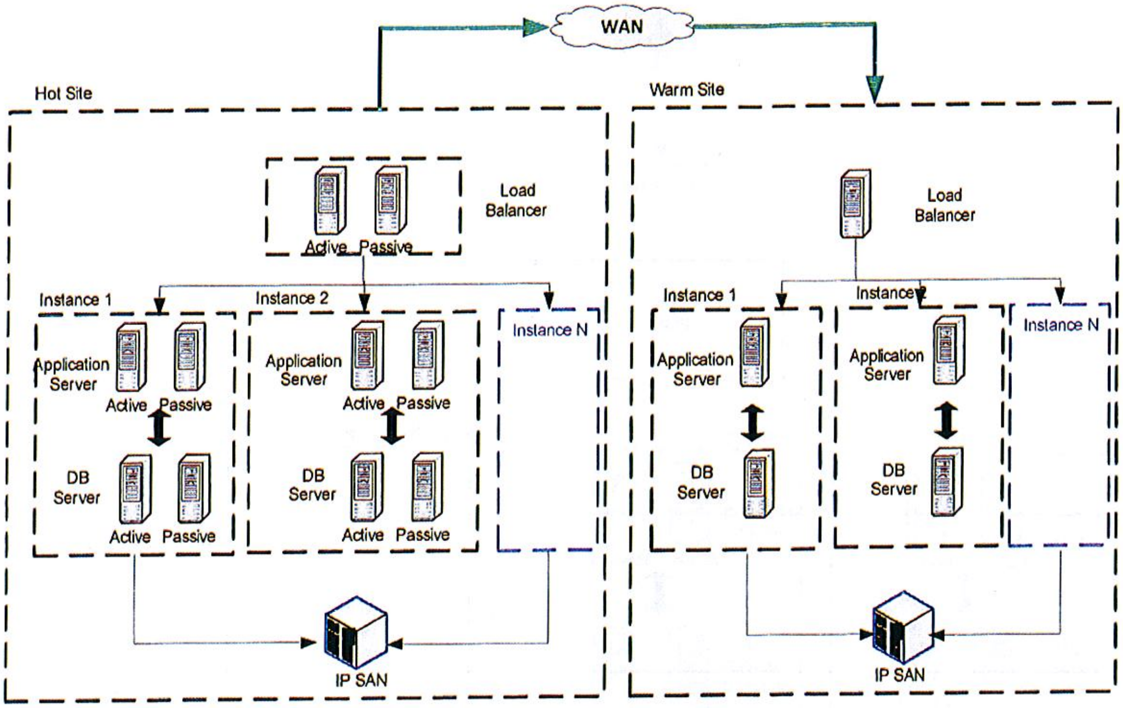


Figure 2: Option 2 Architecture (Offsite DR)

Multi-Site Infrastructure:

- Multi-site infrastructure redundancy
- Application fail over cluster
- DB Server failover cluster
- Clustered SAN Devices
- Dual IP SAN switches

Practice without Boundaries

CureMD is the leading provider of Cloud based EHR, Practice Management and Medical Billing services to transform the administrative and clinical operations of healthcare organizations of all sizes. Our award winning solutions simplify decision making, streamline operations and ensure compliance with industry standards and best practices ultimately saving time and effort to maximize value and returns.

CureMD Healthcare
120 Broadway, 35th Floor
New York, NY 10271
Phone: +1 (866) 643 836
www.curemd.com

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (hereinafter referred to as "**the Agreement**") is being made and entered into on 7th day of January, 2016 as an integral part of the Services Agreement (as defined below), by and between:

Guilford County Department of Health and Human Services located at 1203 Maple Street, Greensboro, NC 27405 (hereinafter referred to as "**Covered Entity**")

AND

CureMD.com, Inc., a New York corporation, having its principal place of business at 120 Broadway, New York, NY 10271 (hereinafter referred to as "**Business Associate**")

(Both Covered Entity and Business Associate would also be referred as "Party" individually and collectively as "Parties" herein below)

RECITALS

WHEREAS, Covered Entity and Business Associate are Parties to the Services Agreement pursuant to which Business Associate provides certain services to Covered Entity. While providing services, Business Associate creates or receives Protected Health Information from or on behalf of Covered Entity, which information is subject to protection under Federal Health Insurance Portability and Accountability Act of 1996 (hereinafter "**HIPAA**"), the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (hereinafter "**HITECH Act**"), and related regulations promulgated by the Secretary (hereinafter "**HIPAA Regulations**");

WHEREAS, in light of the foregoing and the requirements under HIPAA, the HITECH Act and the HIPAA Regulations, both parties are hereby bound by the terms and obligations provided herein below;

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. DEFINITIONS:

   a. General: Terms used, but not otherwise defined, in this Agreement shall have the same meaning given to those terms by HIPAA, the HITECH Act and HIPAA Regulations as in effect or as amended from time to time.

   b. Specific:

      i. Breach shall have the same meaning as per the term 'breach' enshrined under the HITECH Act, Section 13400(1).

      ii. Electronic Health Record shall have the same meaning as per the term 'electronic health record' enshrined under the HITECH Act, Section 13400(5).

      iii. Electronic Protected Health Information shall have the same meaning as per the term 'electronic protected health information' provided under 45 CFR § 160.103, limited to the information that Business Associate creates, receives, maintains or transmits for or on behalf of Covered Entity.

iv. Individual shall have the same meaning as per the term 'individual' given under 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

v. Privacy Rule shall have the same meaning the Standards of Privacy of Individually Identifiable Health Information at 45 CFR Part 160, Part 162 and Part 164.

vi. Protected Health Information shall have the same meaning as per the term 'protected health information' provided under 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. Notwithstanding the foregoing, Protected Health Information shall include such information that is included in 'Data' created or received by Business Associate as such term may be defined under any Services Agreement.

vii. Designated Record Set shall mean those records maintained by Business Associate, including the medical and billing records about Individuals, in addition to any enrollment, payment, claims adjudication and case or medical management record systems.

viii. Required by Law shall have the same meaning as per the term 'required by law' in 45 CFR § 164.103.

ix. Secretary shall mean the Secretary of the Department of Health and Human Services or his designee.

x. Security Rule shall mean the Security Standards at 45 CFR Part 160 and Part 164.

xi. Services Agreement shall mean (i) any present or future agreements, either written or oral, between Covered Entity and Business Associate under which Business Associate provides services to Covered Entity which involve the use or disclosure of Protected Health Information, and (ii) certain Services Agreement executed between the Covered Entity and Business Associate, effective as of _________. The Services Agreement is amended by and incorporates the terms of this Agreement and subsequently this Agreement is deemed an integral part thereof.

xii. Unsecured Protected Health Information shall have the same meaning as per the term provided in the HITECH Act, Section 13402(h)(1).

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

a. Use and Disclosure: Business Associate agrees not to use or disclose Protected Health Information (hereinafter "PHI") other than as permitted or required by the Services Agreement, this Agreement or as required by Law.

b. Appropriate Safeguards: Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of the PHI other than as provided for by this Agreement. Without limiting the generality of the aforementioned, Business Associate shall:

i. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information as required by the Security Rule;

ii. Ensure that any agent, including a subcontractor, to whom Business Associate provides Electronic Protected Health Information agrees to implement reasonable and appropriate safeguards to protect Electronic Protected Health Information;

iii. Promptly report to Covered Entity regarding any Security Incident of which Business Associate becomes aware. In addition, Business Associate agrees to promptly notify Covered Entity following the discovery of a Breach of Unsecured Protected Health Information. A Breach shall be considered as 'discovered' on the first day the Breach is known, or reasonably ought to have been known, to Business Associate or any of its employees, officers or agents, other than the individual committing the Breach. Any notice of a Security Incident or Breach of Unsecured Protected Health Information shall include the identification of each individual whose PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Security Incident or Breach as well as any other relevant information regarding the Security Incident or Breach.

c. Reporting: Business Associate agrees to promptly report to Covered Entity any use or disclosure of PHI not permitted by this Agreement of which Business Associate becomes aware.

d. Mitigation: Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its employees, officers or agents in violation of the requirements of this Agreement (including, without limitation, any Security Incident or Breach of Unsecured Protected Health Information). Business Associate agrees to reasonably cooperate and coordinate with Covered Entity in the investigation of any violation of the requirements of this Agreement and / or any Security Incident or Breach. Business Associate shall also reasonably cooperate and coordinate with Covered Entity in the preparation of any notices or reports to the Individual, a regulatory body or any third party required to be made under HIPAA, the HIPAA Regulations, the HITECH Act, or any other Federal or State Laws, rules or regulations.

e. Agents and Subcontractors: Business Associate shall ensure that any agent, including a sub-contractor, to whom it provides PHI received from, or created by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f. Access to Designated Record Sets: To the extent that Business Associate possesses or maintains PHI in Designated Record Sets, Business Associate agrees to provide access to such Designated Record Sets at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity, to an Individual in order to comply with the requirements given under the HIPAA Regulations. If an Individual makes a request for access to PHI directly to Business Associate, it shall notify Covered Entity within three (3) business days of such a request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

g. Amendments to Designated Record Sets: To the extent that Business Associate possesses or maintains PHI in Designated Record Sets, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to HIPAA Regulations at the request of Covered Entity or an Individual, and in the time and manner reasonably designated by Covered Entity. If an Individual makes a request for an amendment to PHI directly to Business Associate, it shall notify Covered Entity within ten (10) business days of such a request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

h. Access to Books and Records: Business Associate agrees to make its internal practices, books and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate, on behalf of Covered Entity, available to the Covered Entity, or to the Secretary in the time and manner designated by the Covered Entity or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

i. Accounting: Business Associate agrees to document such disclosures of PHI and information pertaining to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with HIPAA, HIPAA Regulations and the HITECH Act, as of its effective date.

j. Requests for Accounting: Business Associate agrees to provide to Covered Entity or an Individual, in the time and manner designated by the Covered Entity, information collected in accordance with Clause 2(i) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with HIPAA, HIPAA Regulations and the HITECH Act, as of its effective date. If an Individual makes a request for an accounting directly from the Business Associate, it shall notify Covered Entity of the request within ten (10) business days of such request and will cooperate with Covered Entity to send the response to the Individual.

k. Forwarding Individual's Requests: If forwarding the individual's request for access to, amendment of, or accounting of PHI to Covered Entity would cause the Business Associate to violate the HIPAA, HIPAA Regulations or the HITECH Act, the Business Associate shall instead respond to the individual's request as required by such law and notify the Covered Entity of such a response as soon as practicable.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

a. Services Agreement: Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for or on behalf of, Covered Entity as specified in the Services Agreement, provided that such use or disclosure would not violate HIPAA, HIPAA Regulations or the HITECH Act as of its effective date if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

b. Use for Administration of Business Associate: Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

c. Disclosure for Administration of Business Associate: Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI for the proper management of Business Associate, provided that (a) disclosures are required by Law, or (b) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

d. Permissible requests by Covered Entity: Except as set forth in this Clause 3 of this Agreement, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

4. OBLIGATIONS OF COVERED ENTITY.

a. Notice of Privacy Practices: Covered Entity agrees to provide individuals with notice of its privacy practices and obtain acknowledgment of receipt thereof in compliance with 45 C.F.R. § 164.520. In addition, upon request Covered Entity shall promptly provide Business Associate with a copy of its privacy practices in accordance with 45 C.F.R. § 164.520, as well as any modifications thereto.

b. Changes In or Revocation of Permission by Individuals: Covered Entity shall promptly notify Business Associate, in writing, of any changes in, or revocation of, an individual's permission to use or disclose PHI, if such changes or revocation affects Business Associate's permitted or required uses and disclosures.

c. Covered Entity's Agreements to Restrict Use or Disclosure: In the event Covered Entity agrees to restrict the use and/or disclosure of PHI in accordance with 45 C.F.R. § 164.522, it shall promptly notify Business Associate, in writing, of the nature and extent of said restriction. The Covered Entity shall not agree to restrictions on the use or disclosure of PHI that might adversely affect the Business Associate, its ability to perform under the Services Agreement or increase the costs of such performance. The Covered Entity shall notify the Business Associate of any such restrictions that the Covered Entity may have entered into prior to the execution of this Agreement. If any such restrictions exist prior to the execution of the Agreement, the Business Associate shall recover costs that are associated with such restrictions.

d. Permissible Requests by Covered Entity: Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under HIPAA or other applicable law or regulation governing the privacy of PHI.

e. Consents and Authorizations: Covered Entity represents and warrants that any and all consents, authorizations, or other permissions required by HIPAA or other applicable law (including state law) necessary to allow Business Associate to perform the administrative functions, services, or activities on behalf of Covered Entity consistent with this Agreement have been properly secured.

f. Third Party Access: By granting access to third parties outside the United States of America access to the Business Associate's products or services, the Covered Entity accepts and agrees to the Business Associate's Release Agreement for Third Party Access.

5. TERM AND TERMINATION

a. Term: This Agreement shall be effective as of the date mentioned on this Agreement and shall terminate when all underlying agreements between the parties terminate and the parties cease to have an ongoing business relationship.

b. Termination for Cause:

a. In the event a party fails to perform the obligations under this Agreement (the "Breaching Party"), the non-breaching party may, at its option:

i. Require the Breaching Party to submit to a plan of compliance, including monitoring by Non-Breaching Party and reporting by the Breaching Party, as the Non-Breaching Party, in its sole discretion, determines necessary to maintain compliance with this Agreement and applicable law. Such plan shall be incorporated into this Agreement by amendment hereto; and

ii. In case of breach by the Business Associate, immediately discontinue providing PHI to Business Associate with or without written notice to Business Associate.

iii. Furthermore, the Non-Breaching Party may immediately terminate this Agreement and related agreements if the Non-Breaching Party determines that Breaching Party has breached a material term of this Agreement.

iv. Alternatively, Non-Breaching Party may choose to (i) provide Breaching Party with ten (10) days written notice of the existence of an alleged material breach; and (ii) afford Breaching Party an opportunity to cure said alleged material breach to the satisfaction of Non-Breaching Party within (10) days. Breaching Party's failure to cure shall be grounds for immediate termination of this agreement. Non-Breaching Party's remedies under this Agreement are cumulative, and the exercise of any remedy shall not preclude the exercise of any other.

c. Effect of Termination:

i. Except as provided in Clause 5(c)(ii), upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall not retain any copies of PHI whatsoever.

ii. Notwithstanding the foregoing, in the event that Business Associate reasonably determines that returning or destroying the PHI is not feasible, Business Associate shall provide Covered Entity a notification of the conditions that make the return or destruction infeasible, and Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return and destruction infeasible, for as long as Business Associate maintains such PHI.

6. COMPLIANCE WITH HIPAA STANDARDS

To the extent applicable when providing its services and/or products, Business Associate shall comply with all HIPAA Standards and requirements (including, without limitation, those specified in 45 CFR Part 162) with respect to the transmission of health information in electronic form in connection with any transaction for which the Secretary has adopted a standard under HIPAA ("Covered Transactions"). Business Associate will make its services and/or products compliant with HIPAA's Standards and requirements no less than thirty (30) days prior to the applicable compliance dates under HIPAA. Business Associate represents and warrants that it is aware of all current HIPAA Standards regarding Covered Transactions, and Business Associate shall comply with any modifications to HIPAA Standards which become effective from time to time. Business Associate agrees that such compliance shall be at its sole cost and expense, which expense shall not be passed on to Covered Entity in any form, including but not limited to, increased fees. Business Associate shall require all of its agents and subcontractors (if any) who assist in providing its services and/or products to comply with the terms provided herein.

7. MISCELLANEOUS

a. Assignment of Rights and Delegation of Duties: This Agreement is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns. However, neither Party may assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Assignments made in violation of this provision are null and void.

b. Regulatory References: A reference in this Agreement to a Clause in HIPAA, HIPAA Regulations or the HITECH Act means the section as in effect or as amended from time to time, for which compliance is required.

c. Amendment: The Parties agree to take such action as is necessary to amend the Services Agreement from time to time as is necessary for Covered Entity to comply with the requirements of HIPAA, the HIPAA Regulations and the HITECH Act.

d. Survival: The respective rights and obligations of Business Associate as per Clause 5(c) of this Agreement shall survive the termination of the Services Agreement or this Agreement.

e. Interpretation: Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with HIPAA, HIPAA Regulations and the HITECH Act.

f. Indemnification: Covered Entity shall, to the fullest extent permitted by law, protect, defend, indemnify and hold harmless Business Associate and its respective employees, directors, and agents from and against any and all losses, costs, claims, penalties, fines, demands, liabilities, legal actions, judgments, and expenses of every kind (including reasonable attorney's fees, including at trial and on appeal) asserted or imposed against the Business Associate arising out of the acts or omissions of Covered Entity or any of its employees, directors, or agents related to the performance or nonperformance of this Agreement.

g. Severability: The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

h. Miscellaneous: The terms of this Agreement are hereby incorporated into the Services Agreement. In the event of a conflict between the terms of this Agreement and the Services Agreement, the terms of this Agreement shall prevail as it pertains to the subject matter herein. This Agreement shall be governed by, and construed in accordance with the laws of the State of New York, exclusive of conflict of law rules. Each party to this Agreement hereby agrees and consents that any legal action or proceeding with respect to this Agreement shall only be brought in the Courts of the State where the Covered Entity is located. The Services Agreement together with this Agreement constitutes the entire agreement between the parties with respect to the subject matter contained herein, and this Agreement supersedes and replaces any former Business Associate Agreement or Addendum entered into by the Parties. No modifications or amendments to this Agreement shall be deemed effective unless executed by both Parties in writing.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date set forth herein above.

GUILFORD COUNTY, on behalf of the **Guilford County Department of Health and Human Services**, Division of Public Health		**CureMD.com, Inc.**	
Signature:	______________	Signature:	______________
Name:	Marty K. Lawing	Name:	______________
Designation:	Guilford County Manager	Designation:	______________
Date:	______________	Date:	______________
ATTEST:	______________ Guilford County Clerk to Board (COUNTY SEAL)	ATTEST:	______________ Corporate Secretary (CORPORATE SEAL)

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (hereinafter referred to as "**the Agreement**") is being made and entered into on 7th day of January, 2016 as an integral part of the Services Agreement (as defined below), by and between:

Guilford County Department of Health and Human Services located at 1203 Maple Street, Greensboro, NC 27405 (hereinafter referred to as "**Covered Entity**")

AND

Carolinas IT, a North Carolina corporation, having its principal place of business at 1600 Hillsborough Street Raleigh, North Carolina, 27605 (hereinafter referred to as **"Business Associate"**)

(Both Covered Entity and Business Associate would also be referred as "Party" individually and collectively as "Parties" herein below)

RECITALS

WHEREAS, Covered Entity and Business Associate are Parties to the Services Agreement pursuant to which Business Associate provides certain services to Covered Entity. While providing services, Business Associate creates or receives Protected Health Information from or on behalf of Covered Entity, which information is subject to protection under Federal Health Insurance Portability and Accountability Act of 1996 (hereinafter "**HIPAA**"), the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (hereinafter **"HITECH Act"**), and related regulations promulgated by the Secretary (hereinafter **"HIPAA Regulations"**);

WHEREAS, in light of the foregoing and the requirements under HIPAA, the HITECH Act and the HIPAA Regulations, both parties are hereby bound by the terms and obligations provided herein below;

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. DEFINITIONS:

   a. General: Terms used, but not otherwise defined, in this Agreement shall have the same meaning given to those terms by HIPAA, the HITECH Act and HIPAA Regulations as in effect or as amended from time to time.

   b. Specific:

      i. Breach shall have the same meaning as per the term 'breach' enshrined under the HITECH Act, Section 13400(1).

      ii. Electronic Health Record shall have the same meaning as per the term 'electronic health record' enshrined under the HITECH Act, Section 13400(5).

      iii. Electronic Protected Health Information shall have the same meaning as per the term 'electronic protected health information' provided under 45 CFR § 160.103, limited to the information that Business Associate creates, receives, maintains or transmits for or on behalf of Covered Entity.

iv. Individual shall have the same meaning as per the term 'individual' given under 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

v. Privacy Rule shall have the same meaning the Standards of Privacy of Individually Identifiable Health Information at 45 CFR Part 160, Part 162 and Part 164.

vi. Protected Health Information shall have the same meaning as per the term 'protected health information' provided under 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. Notwithstanding the foregoing, Protected Health Information shall include such information that is included in 'Data' created or received by Business Associate as such term may be defined under any Services Agreement.

vii. Designated Record Set shall mean those records maintained by Business Associate, including the medical and billing records about Individuals, in addition to any enrollment, payment, claims adjudication and case or medical management record systems.

viii. Required by Law shall have the same meaning as per the term 'required by law' in 45 CFR § 164.103.

ix. Secretary shall mean the Secretary of the Department of Health and Human Services or his designee.

x. Security Rule shall mean the Security Standards at 45 CFR Part 160 and Part 164.

xi. Services Agreement shall mean (i) any present or future agreements, either written or oral, between Covered Entity and Business Associate under which Business Associate provides services to Covered Entity which involve the use or disclosure of Protected Health Information, and (ii) certain Services Agreement executed between the Covered Entity and Business Associate, effective as of _________. The Services Agreement is amended by and incorporates the terms of this Agreement and subsequently this Agreement is deemed an integral part thereof.

xii. Unsecured Protected Health Information shall have the same meaning as per the term provided in the HITECH Act, Section 13402(h)(1).

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

a. Use and Disclosure: Business Associate agrees not to use or disclose Protected Health Information (hereinafter **"PHI"**) other than as permitted or required by the Services Agreement, this Agreement or as required by Law.

b. Appropriate Safeguards: Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of the PHI other than as provided for by this Agreement. Without limiting the generality of the aforementioned, Business Associate shall:

i. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information as required by the Security Rule;

ii. Ensure that any agent, including a subcontractor, to whom Business Associate provides Electronic Protected Health Information agrees to implement reasonable and appropriate safeguards to protect Electronic Protected Health Information;

iii. Promptly report to Covered Entity regarding any Security Incident of which Business Associate becomes aware. In addition, Business Associate agrees to promptly notify Covered Entity following the discovery of a Breach of Unsecured Protected Health Information. A Breach shall be considered as 'discovered' on the first day the Breach is known, or reasonably ought to have been known, to Business Associate or any of its employees, officers or agents, other than the individual committing the Breach. Any notice of a Security Incident or Breach of Unsecured Protected Health Information shall include the identification of each individual whose PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Security Incident or Breach as well as any other relevant information regarding the Security Incident or Breach.

c. Reporting: Business Associate agrees to promptly report to Covered Entity any use or disclosure of PHI not permitted by this Agreement of which Business Associate becomes aware.

d. Mitigation: Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its employees, officers or agents in violation of the requirements of this Agreement (including, without limitation, any Security Incident or Breach of Unsecured Protected Health Information). Business Associate agrees to reasonably cooperate and coordinate with Covered Entity in the investigation of any violation of the requirements of this Agreement and / or any Security Incident or Breach. Business Associate shall also reasonably cooperate and coordinate with Covered Entity in the preparation of any notices or reports to the Individual, a regulatory body or any third party required to be made under HIPAA, the HIPAA Regulations, the HITECH Act, or any other Federal or State Laws, rules or regulations.

e. Agents and Subcontractors: Business Associate shall ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f. Access to Designated Record Sets: To the extent that Business Associate possesses or maintains PHI in Designated Record Sets, Business Associate agrees to provide access to such Designated Record Sets at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity, to an Individual in order to comply with the requirements given under the HIPAA Regulations. If an Individual makes a request for access to PHI directly to Business Associate, it shall notify Covered Entity within three (3) business days of such a request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

g. Amendments to Designated Record Sets: To the extent that Business Associate possesses or maintains PHI in Designated Record Sets, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to HIPAA Regulations at the request of Covered Entity or an Individual, and in the time and manner reasonably designated by Covered Entity. If an Individual makes a request for an amendment to PHI directly to Business Associate, it shall notify Covered Entity within ten (10) business days of such a request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

h. Access to Books and Records: Business Associate agrees to make its internal practices, books and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate, on behalf of Covered Entity, available to the Covered Entity, or to the Secretary in the time and manner designated by the Covered Entity or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

i. Accounting: Business Associate agrees to document such disclosures of PHI and information pertaining to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with HIPAA, HIPAA Regulations and the HITECH Act, as of its effective date.

j. Requests for Accounting: Business Associate agrees to provide to Covered Entity or an Individual, in the time and manner designated by the Covered Entity, information collected in accordance with Clause 2(i) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with HIPAA, HIPAA Regulations and the HITECH Act, as of its effective date. If an Individual makes a request for an accounting directly from the Business Associate, it shall notify Covered Entity of the request within ten (10) business days of such request and will cooperate with Covered Entity to send the response to the Individual.

k. Forwarding Individual's Requests: If forwarding the individual's request for access to, amendment of, or accounting of PHI to Covered Entity would cause the Business Associate to violate the HIPAA, HIPAA Regulations or the HITECH Act, the Business Associate shall instead respond to the individual's request as required by such law and notify the Covered Entity of such a response as soon as practicable.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

a. Services Agreement: Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for or on behalf of, Covered Entity as specified in the Services Agreement, provided that such use or disclosure would not violate HIPAA, HIPAA Regulations or the HITECH Act as of its effective date if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

b. Use for Administration of Business Associate: Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

c. Disclosure for Administration of Business Associate: Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI for the proper management of Business Associate, provided that (a) disclosures are required by Law, or (b) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

d. Permissible requests by Covered Entity: Except as set forth in this Clause 3 of this Agreement, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

4. OBLIGATIONS OF COVERED ENTITY.

a. Notice of Privacy Practices: Covered Entity agrees to provide individuals with notice of its privacy practices and obtain acknowledgment of receipt thereof in compliance with 45 C.F.R. § 164.520. In addition, upon request Covered Entity shall promptly provide Business Associate with a copy of its privacy practices in accordance with 45 C.F.R. § 164.520, as well as any modifications thereto.

b. Changes In or Revocation of Permission by Individuals: Covered Entity shall promptly notify Business Associate, in writing, of any changes in, or revocation of, an individual's permission to use or disclose PHI, if such changes or revocation affects Business Associate's permitted or required uses and disclosures.

c. Covered Entity's Agreements to Restrict Use or Disclosure: In the event Covered Entity agrees to restrict the use and/or disclosure of PHI in accordance with 45 C.F.R. § 164.522, it shall promptly notify Business Associate, in writing, of the nature and extent of said restriction. The Covered Entity shall not agree to restrictions on the use or disclosure of PHI that might adversely affect the Business Associate, its ability to perform under the Services Agreement or increase the costs of such performance. The Covered Entity shall notify the Business Associate of any such restrictions that the Covered Entity may have entered into prior to the execution of this Agreement. If any such restrictions exist prior to the execution of the Agreement, the Business Associate shall recover costs that are associated with such restrictions.

d. Permissible Requests by Covered Entity: Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under HIPAA or other applicable law or regulation governing the privacy of PHI.

e. Consents and Authorizations: Covered Entity represents and warrants that any and all consents, authorizations, or other permissions required by HIPAA or other applicable law (including state law) necessary to allow Business Associate to perform the administrative functions, services, or activities on behalf of Covered Entity consistent with this Agreement have been properly secured.

f. Third Party Access: By granting access to third parties outside the United States of America access to the Business Associate's products or services, the Covered Entity accepts and agrees to the Business Associate's Release Agreement for Third Party Access.

5. TERM AND TERMINATION

a. Term: This Agreement shall be effective as of the date mentioned on this Agreement and shall terminate when all underlying agreements between the parties terminate and the parties cease to have an ongoing business relationship.

b. Termination for Cause:

a. In the event a party fails to perform the obligations under this Agreement (the "Breaching Party"), the non-breaching party may, at its option:

i. Require the Breaching Party to submit to a plan of compliance, including monitoring by Non-Breaching Party and reporting by the Breaching Party, as the Non-Breaching Party, in its sole discretion, determines necessary to maintain compliance with this Agreement and applicable law. Such plan shall be incorporated into this Agreement by amendment hereto; and

ii. In case of breach by the Business Associate, immediately discontinue providing PHI to Business Associate with or without written notice to Business Associate.

iii. Furthermore, the Non-Breaching Party may immediately terminate this Agreement and related agreements if the Non-Breaching Party determines that Breaching Party has breached a material term of this Agreement.

iv. Alternatively, Non-Breaching Party may choose to (i) provide Breaching Party with ten (10) days written notice of the existence of an alleged material breach; and (ii) afford Breaching Party an opportunity to cure said alleged material breach to the satisfaction of Non-Breaching Party within (10) days. Breaching Party's failure to cure shall be grounds for immediate termination of this agreement. Non-Breaching Party's remedies under this Agreement are cumulative, and the exercise of any remedy shall not preclude the exercise of any other.

c. Effect of Termination:

i. Except as provided in Clause 5(c)(ii), upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall not retain any copies of PHI whatsoever.

ii. Notwithstanding the foregoing, in the event that Business Associate reasonably determines that returning or destroying the PHI is not feasible, Business Associate shall provide Covered Entity a notification of the conditions that make the return or destruction infeasible, and Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return and destruction infeasible, for as long as Business Associate maintains such PHI.

6. COMPLIANCE WITH HIPAA STANDARDS

To the extent applicable when providing its services and/or products, Business Associate shall comply with all HIPAA Standards and requirements (including, without limitation, those specified in 45 CFR Part 162) with respect to the transmission of health information in electronic form in connection with any transaction for which the Secretary has adopted a standard under HIPAA ("Covered Transactions"). Business Associate will make its services and/or products compliant with HIPAA's Standards and requirements no less than thirty (30) days prior to the applicable compliance dates under HIPAA. Business Associate represents and warrants that it is aware of all current HIPAA Standards regarding Covered Transactions, and Business Associate shall comply with any modifications to HIPAA Standards which become effective from time to time. Business Associate agrees that such compliance shall be at its sole cost and expense, which expense shall not be passed on to Covered Entity in any form, including but not limited to, increased fees. Business Associate shall require all of its agents and subcontractors (if any) who assist in providing its services and/or products to comply with the terms provided herein.

7. MISCELLANEOUS

a. Assignment of Rights and Delegation of Duties: This Agreement is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns. However, neither Party may assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Assignments made in violation of this provision are null and void.

b. Regulatory References: A reference in this Agreement to a Clause in HIPAA, HIPAA Regulations or the HITECH Act means the section as in effect or as amended from time to time, for which compliance is required.

c. Amendment: The Parties agree to take such action as is necessary to amend the Services Agreement from time to time as is necessary for Covered Entity to comply with the requirements of HIPAA, the HIPAA Regulations and the HITECH Act.

d. Survival: The respective rights and obligations of Business Associate as per Clause 5(c) of this Agreement shall survive the termination of the Services Agreement or this Agreement.

e. Interpretation: Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with HIPAA, HIPAA Regulations and the HITECH Act.

f. Indemnification: Covered Entity shall, to the fullest extent permitted by law, protect, defend, indemnify and hold harmless Business Associate and its respective employees, directors, and agents from and against any and all losses, costs, claims, penalties, fines, demands, liabilities, legal actions, judgments, and expenses of every kind (including reasonable attorney's fees, including at trial and on appeal) asserted or imposed against the Business Associate arising out of the acts or omissions of Covered Entity or any of its employees, directors, or agents related to the performance or nonperformance of this Agreement.

g. Severability: The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

h. Miscellaneous: The terms of this Agreement are hereby incorporated into the Services Agreement. In the event of a conflict between the terms of this Agreement and the Services Agreement, the terms of this Agreement shall prevail as it pertains to the subject matter herein. This Agreement shall be governed by, and construed in accordance with the laws of the State of North Carolina, exclusive of conflict of law rules. Each party to this Agreement hereby agrees and consents that any legal action or proceeding with respect to this Agreement shall only be brought in the Courts of the State where the Covered Entity is located. The Services Agreement together with this Agreement constitutes the entire agreement between the parties with respect to the subject matter contained herein, and this Agreement supersedes and replaces any former Business Associate Agreement or Addendum entered into by the Parties. No modifications or amendments to this Agreement shall be deemed effective unless executed by both Parties in writing.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date set forth herein above.

GUILFORD COUNTY, on behalf of the **Guilford County Department of** **Health and Human Services**, Public Health Division		**Carolinas IT**	
Signature:	______________________	Signature:	______________________
Name:	Marty K. Lawing	Name:	______________________
Designation:	Guilford County Manager	Designation:	____________________
Date:	______________________	Date:	______________________

ATTEST:____________________________
Guilford County Clerk to Board
(COUNTY SEAL)

ATTEST:____________________________
Corporate Secretary
(CORPORATE SEAL)

ATTACHMENT B - GUILFORD COUNTY CONTRACT NO. 113348-03/16-271
CAROLINAS IT, INC. (PROVIDER)

Form **W-9**
(Rev. December 2011)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

Give Form to the requester. Do not send to the IRS.

Print or type
See Specific Instructions on page 2.

Name (as shown on your income tax return)
Carolinas IT, Inc.

Business name/disregarded entity name, if different from above

Check appropriate box for federal tax classification:
□ Individual/sole proprietor ☑ C Corporation □ S Corporation □ Partnership □ Trust/estate

□ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=partnership) ▶ ....

□ Other (see instructions) ▶

□ Exempt payee

Address (number, street, and apt. or suite no.)
1600 Hillsborough St

City, state, and ZIP code
Raleigh, NC 27605

Requester's name and address (optional)

List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on the "Name" line to avoid backup withholding. For individuals, this is your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the Part I instructions on page 3. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN* on page 3.

Note. If the account is in more than one name, see the chart on page 4 for guidelines on whose number to enter.

Social security number
☐☐☐ - ☐☐ - ☐☐☐☐

Employer identification number
5 6 - 1 9 7 1 8 5 0

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding, and
3. I am a U.S. citizen or other U.S. person (defined below).

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions on page 4.

Sign Here Signature of U.S. person ▶ Amanda L. Abbott Date ▶ 11/02/2012

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Purpose of Form

A person who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) to report, for example, income paid to you, real estate transactions, mortgage interest you paid, acquisition or abandonment of secured property, cancellation of debt, or contributions you made to an IRA.

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN to the person requesting it (the requester) and, when applicable, to:

1. Certify that the TIN you are giving is correct (or you are waiting for a number to be issued),

2. Certify that you are not subject to backup withholding, or

3. Claim exemption from backup withholding if you are a U.S. exempt payee. If applicable, you are also certifying that as a U.S. person, your allocable share of any partnership income from a U.S. trade or business is not subject to the withholding tax on foreign partners' share of effectively connected income.

Note. If a requester gives you a form other than Form W-9 to request your TIN, you must use the requester's form if it is substantially similar to this Form W-9.

Definition of a U.S. person. For federal tax purposes, you are considered a U.S. person if you are:

- An individual who is a U.S. citizen or U.S. resident alien,
- A partnership, corporation, company, or association created or organized in the United States or under the laws of the United States,
- An estate (other than a foreign estate), or
- A domestic trust (as defined in Regulations section 301.7701-7).

Special rules for partnerships. Partnerships that conduct a trade or business in the United States are generally required to pay a withholding tax on any foreign partners' share of income from such business. Further, in certain cases where a Form W-9 has not been received, a partnership is required to presume that a partner is a foreign person, and pay the withholding tax. Therefore, if you are a U.S. person that is a partner in a partnership conducting a trade or business in the United States, provide Form W-9 to the partnership to establish your U.S. status and avoid withholding on your share of partnership income.

MaaS360®
by Fiberlink, an IBM company

TruSaaS™

MaaS360® for Healthcare

MaaS360 in Action: Millions in HIPAA Fines Wiped Clean

A physician relies on an iPhone to access medical reference libraries, patient records and lab results—in addition to calendar scheduling, voice and text messaging. On a speaking engagement abroad, the iPhone is stolen—on a bistro table one minute, gone the next.

Without hesitation, the physician calls the hospital where he is on staff and directs the IT department, equipped with MaaS360, to wipe all information from the device, which is done by the IT department remotely in a matter of minutes.

Protect Patient Information
HIPAA

Healthcare-Specific Challenges

Physicians and healthcare workers increasingly depend on their own mobile devices to access medical and patient data at the point of care. At the same time, healthcare organizations face greater liability and fines if found out of compliance with HIPAA under a new audit program mandated by the 2009 HITECH Act, where the maximum penalty was increased to $1.5 million.

While mobile technology improves the quality and cost of patient care, it increases IT workloads and the potential for information security and HIPAA compliance risks. IT is expected to manage all of these risks while improving the productivity of your healthcare colleagues and keeping them happy by allowing them to use their own mobile devices.

MaaS360 Healthcare Solution

MaaS360 enables organizations to secure electronic protected healthcare information (EPHI) on all mobile devices connecting to their network, comply with HIPAA and other regulations, and reduce the IT workload and cost of managing mobile devices.

Using MaaS360, Mobile Device Management (MDM), Mobile Application Management (MAM), and document and expense management can be easily and instantly integrated into broader enterprise programs for IT governance, data security and regulatory compliance.

[illegible]

- Gain 360° visibility and control of all mobile devices, apps, documents and files
- Automate password, encryption and policy enforcement
- Ensure anytime, anywhere device and data security with immediate remote action on nonconforming devices
- No infrastructure changes required
- Rapid implementation
- Low implementation costs and no-fuss maintenance
- Expense management to control costs and overages

[illegible]

- Supports today's mobile devices from a single console, including iPhone, iPad, Android, Windows Phone, BlackBerry and Kindle Fire
- Instant device enrollment via SMS, email or URL over-the-air (OTA)
- Pushed policies, encryption and security safeguards
- Contextual, event-based policy, security and compliance rules engine and automation
- Enforce usage policies specific to physicians, healthcare workers and staff
- Remote locate, lock and wipe (full and selective)
- Blacklisting, whitelisting and requiring apps
- Customized app catalog
- Support for custom apps
- Control document distribution
- Real-time reporting and analytics

MaaS360
by Fiberlink, an IBM company

MaaS360 for Healthcare

Control All Devices

MaaS360 gives healthcare organizations coordinated visibility and control over all devices and operating systems, from Apple iOS to Android, Windows Phone and BlackBerry. Integrated dashboards, analytics, and reporting provide actionable intelligence about their entire mobile environment through a single console. IT administrators can quickly visualize the distribution of devices, apps and documents across platforms, approval status, device capabilities, ownership, compliance status and more to control the risks of physicians and healthcare workers using mobile devices to access medical apps and patient records.

Improve Mobile Information Security and HIPAA Compliance

MaaS360 provides the ability to know and control information security safeguards on all mobile devices – and react rapidly to lost or stolen devices to ensure regulatory compliance with HIPAA, Health Information Technology for Economic and Clinical Health Act (HITECH), Federal Information Security Management Act (FISMA), Sarbanes-Oxley (SOX), Federal Rules of Civil Procedure (FRCP) and other statutes. IT departments can:

- Push policies and Wi-Fi, email and VPN profiles OTA
- Quarantine new devices automatically until authorized to access your network
- Wipe sensitive data from lost or stolen devices remotely
- Blacklist applications and block device access
- Enforce passcode protection, encryption, and security updates

Control Mobile Applications

MaaS360 application management allows healthcare organizations to easily manage and secure the applications that are critical to your users (e.g. Electronic Health Records (EHR), Computerized Physician Order Entry (CPOE), Diagnostic Imaging, Patient Vitals Monitoring, Point of Care, etc.). An on-device application provides users with a catalog of authorized private and public apps. Users can view the apps made available to them, install apps, and be alerted to updates. IT and other departments can manage the master app catalog and per-user authorization. Application lifecycle management provides real-time software inventory reports, app distribution and installation tracking, update publishing, provisioning profile management, and app security and compliance management.

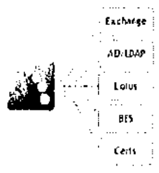
Reduce IT Workload and Costs

With MaaS360's true SaaS model, there are no servers to install, no complex configurations or infrastructure changes, and no investment in expensive business software. Built on a secure, multi-tenant cloud architecture, Maas360 enables instant enterprise mobility management in just minutes with effortless scalability, whether from ten to tens of thousands users, and seamless integration into existing enterprise systems. Additionally, MaaS360 eliminates the strain and expense that rapidly changing mobile devices and applications used by physicians and healthcare workers can have on IT organizations by automatically incorporating the continuous stream of platform updates.

Why MaaS360

Proven approach to cloud-based mobility management

Powerful management & security to address the full mobility lifecycle



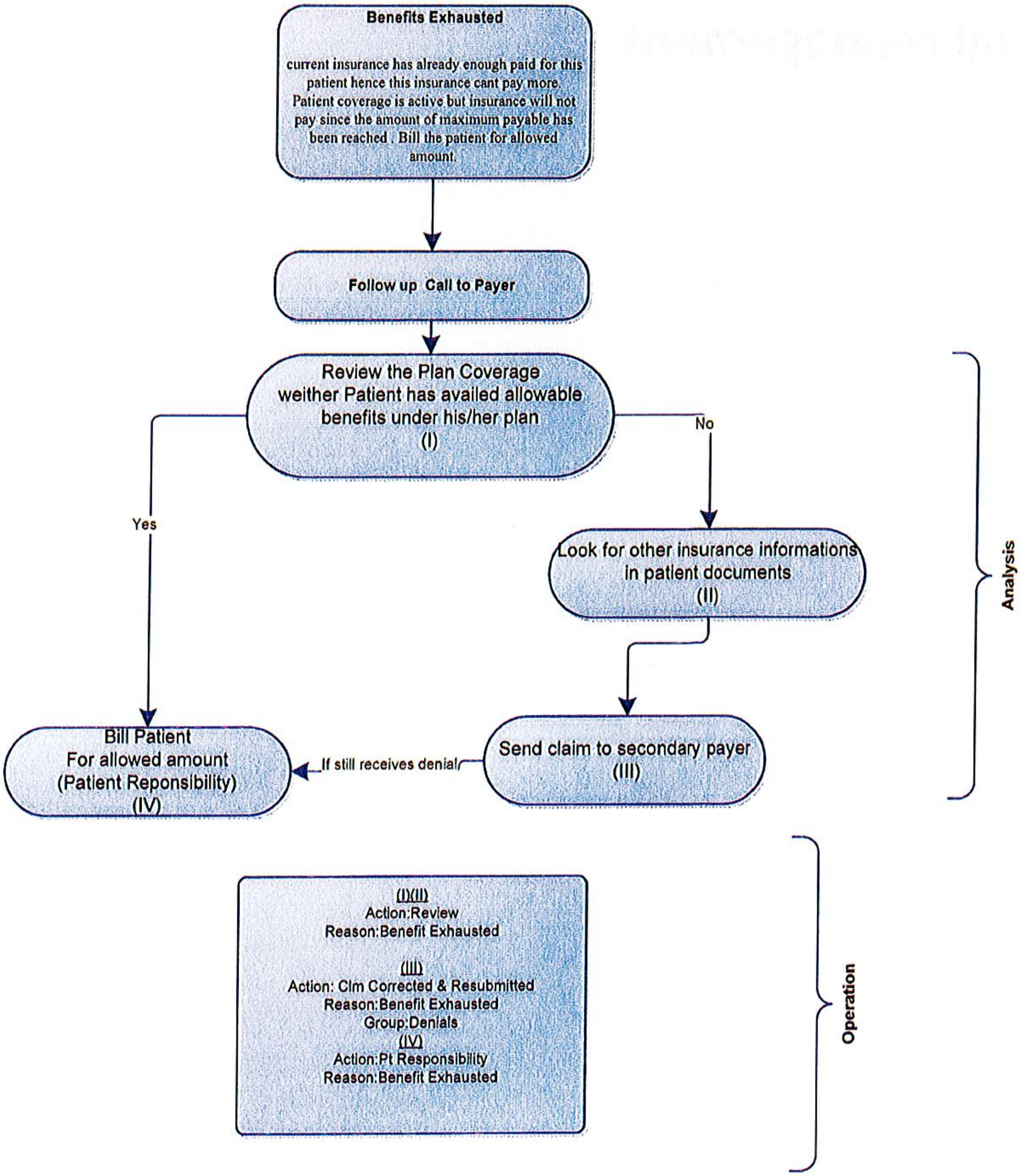
Seamlessly integrates with all of your existing infrastructure

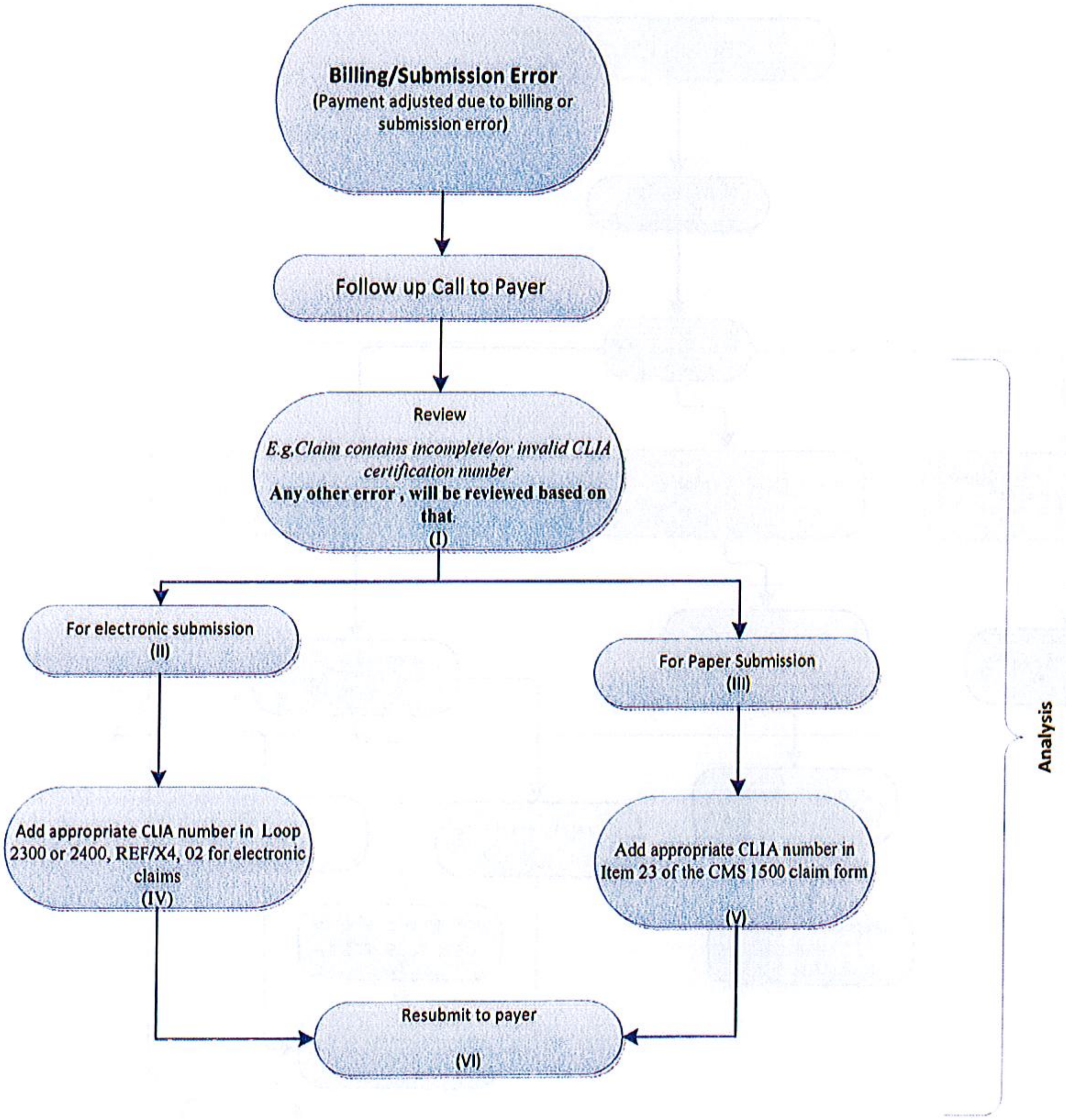
Simple & fast with an exceptional customer experience

For More Information

To learn more about our technology and services contact Carolinas IT
Phone 919.573.4083 | Email info@carolinasit.com

Denial Management

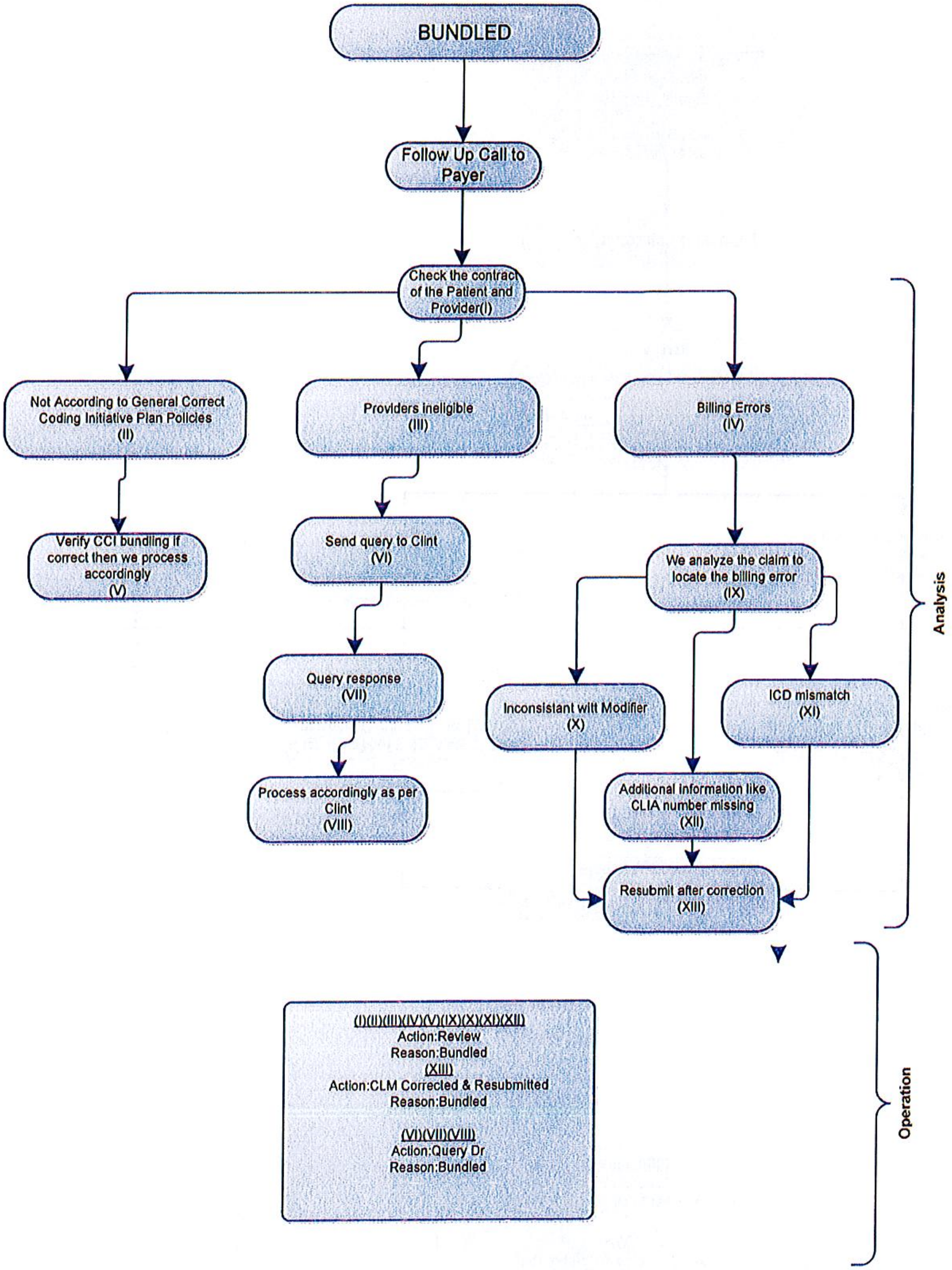

Benefits Exhausted
current insurance has already enough paid for this patient hence this insurance cant pay more. Patient coverage is active but insurance will not pay since the amount of maximum payable has been reached . Bill the patient for allowed amount.
Follow up Call to Payer
Review the Plan Coverage weither Patient has availed allowable benefits under his/her plan (I)
Yes
No
Look for other insurance informations in patient documents (II)
Send claim to secondary payer (III)
If still receives denial
Bill Patient For allowed amount (Patient Reponsibility) (IV)
Analysis
(I)(II)
Action:Review
Reason:Benefit Exhausted
(III)
Action: Clm Corrected & Resubmitted
Reason:Benefit Exhausted
Group:Denials
(IV)
Action:Pt Responsibility
Reason:Benefit Exhausted
Operation

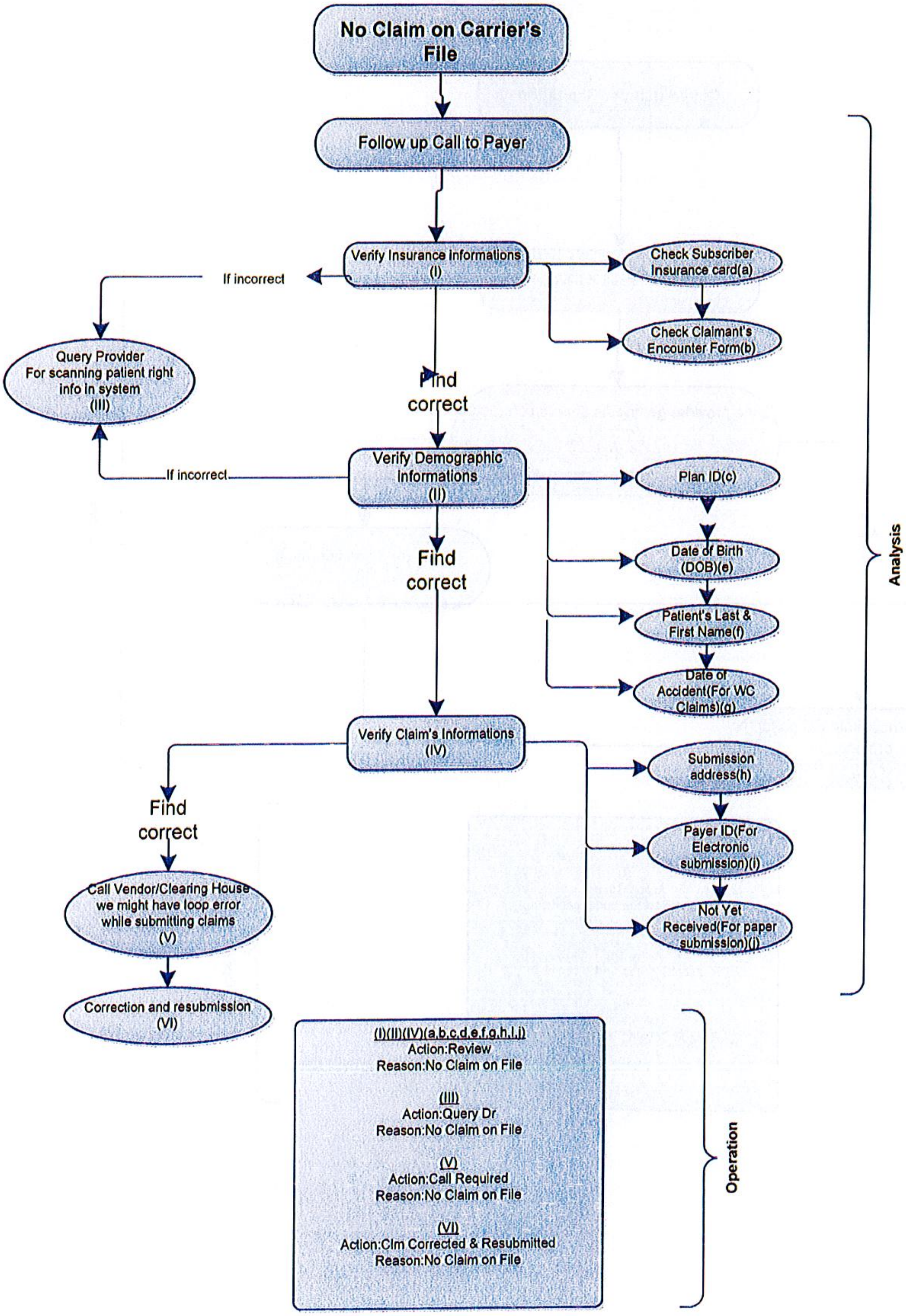

Billing/Submission Error
(Payment adjusted due to billing or submission error)
Follow up Call to Payer
Review
E.g.Claim contains incomplete/or invalid CLIA certification number
Any other error , will be reviewed based on that.
(I)
For electronic submission
(II)
For Paper Submission
(III)
Add appropriate CLIA number in Loop 2300 or 2400, REF/X4, 02 for electronic claims
(IV)
Add appropriate CLIA number in Item 23 of the CMS 1500 claim form
(V)
Resubmit to payer
(VI)
Analysis

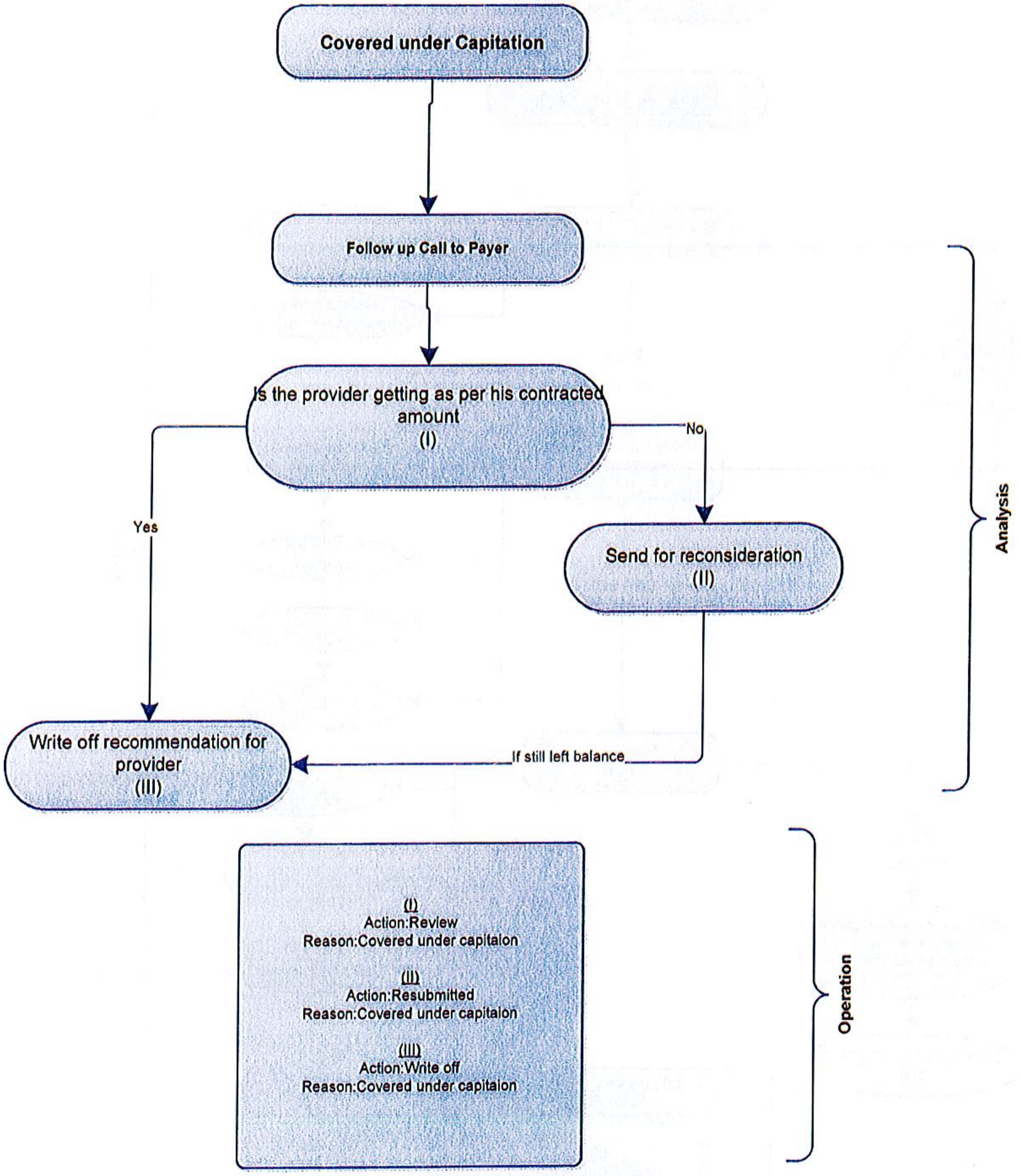
(I)(II)(III)(IV)(V)
Action:REVIEW
Reason:SUBMISSION/BILLING ERROR

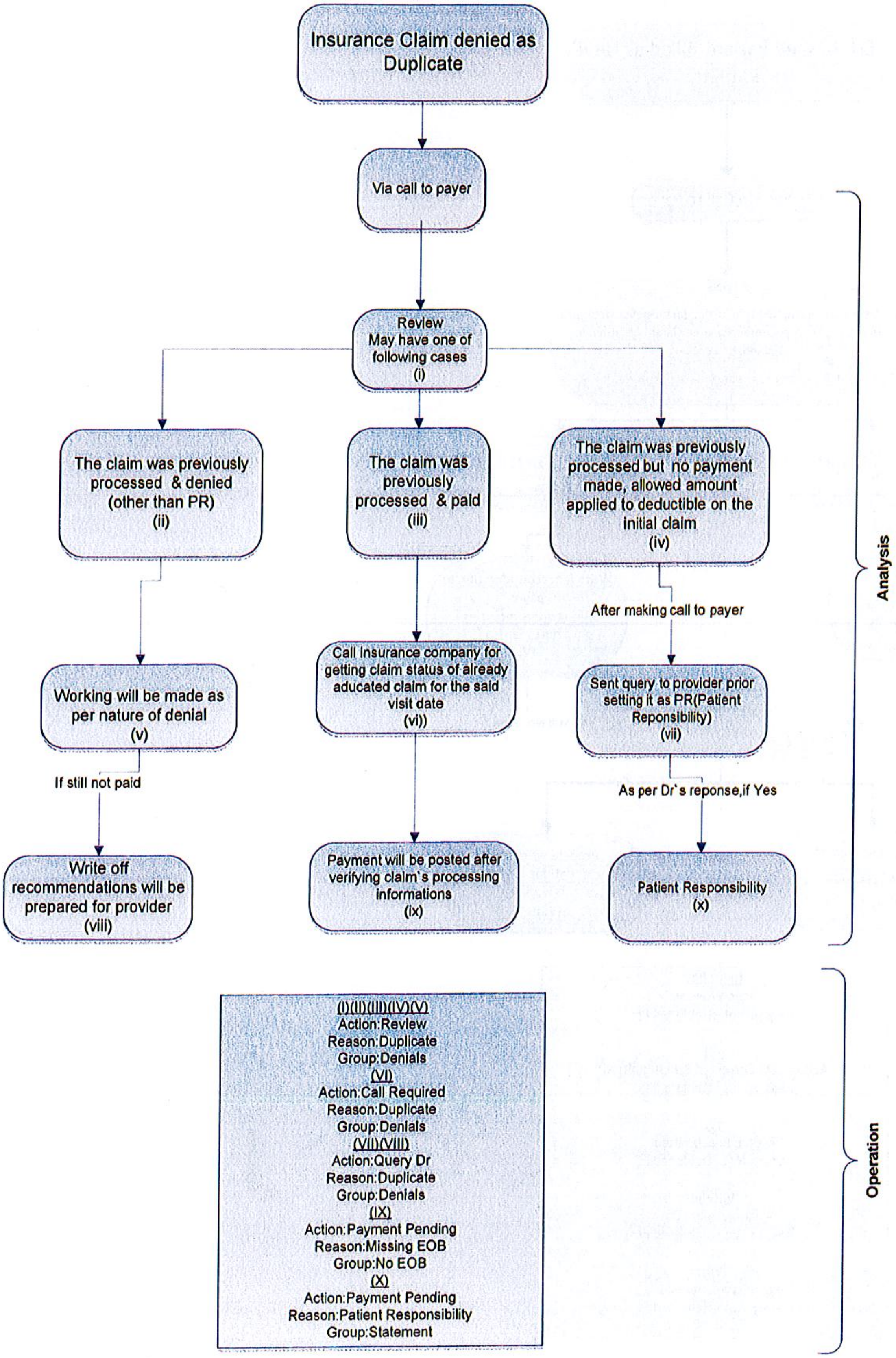
(VI)
Action: Corrected & Resubmitted
Reason:SUBMISSION/BILLING ERROR

Operation


BUNDLED
Follow Up Call to Payer
Check the contract of the Patient and Provider(I)
Not According to General Correct Coding Initiative Plan Policies (II)
Providers Ineligible (III)
Billing Errors (IV)
Verify CCI bundling if correct then we process accordingly (V)
Send query to Clint (VI)
We analyze the claim to locate the billing error (IX)
Query response (VII)
Inconsistant wit Modifier (X)
ICD mismatch (XI)
Process accordingly as per Clint (VIII)
Additional information like CLIA number missing (XII)
Resubmit after correction (XIII)
Analysis
(I)(II)(III)(IV)(V)(IX)(X)(XI)(XII)
Action:Review
Reason:Bundled
(XIII)
Action:CLM Corrected & Resubmitted
Reason:Bundled
(VI)(VII)(VIII)
Action:Query Dr
Reason:Bundled
Operation


No Claim on Carrier's File
Follow up Call to Payer
Verify Insurance informations (I)
If incorrect
Check Subscriber Insurance card(a)
Check Claimant's Encounter Form(b)
Query Provider For scanning patient right info in system (III)
Find correct
Verify Demographic Informations (II)
If incorrect
Plan ID(c)
Date of Birth (DOB)(e)
Patient's Last & First Name(f)
Date of Accident(For WC Claims)(g)
Find correct
Verify Claim's Informations (IV)
Submission address(h)
Payer ID(For Electronic submission)(i)
Not Yet Received(For paper submission)(j)
Find correct
Call Vendor/Clearing House we might have loop error while submitting claims (V)
Correction and resubmission (VI)
Analysis
(I)(II)(IV)(a,b,c,d,e,f,g,h,I,j)
Action:Review
Reason:No Claim on File
(III)
Action:Query Dr
Reason:No Claim on File
(V)
Action:Call Required
Reason:No Claim on File
(VI)
Action:Clm Corrected & Resubmitted
Reason:No Claim on File
Operation


Covered under Capitation
Follow up Call to Payer
Is the provider getting as per his contracted amount (I)
Yes
No
Send for reconsideration (II)
If still left balance
Write off recommendation for provider (III)
Analysis
(I)
Action:Review
Reason:Covered under capitalon
(II)
Action:Resubmitted
Reason:Covered under capitalon
(III)
Action:Write off
Reason:Covered under capitalon
Operation



Insurance Claim denied as Duplicate

Via call to payer

Review
May have one of following cases
(i)

The claim was previously processed & denied (other than PR)
(ii)

The claim was previously processed & paid
(iii)

The claim was previously processed but no payment made, allowed amount applied to deductible on the initial claim
(iv)

After making call to payer

Working will be made as per nature of denial
(v)

Call Insurance company for getting claim status of already aducated claim for the said visit date
(vi))

Sent query to provider prior setting it as PR(Patient Reponsibility)
(vii)

If still not paid

As per Dr`s reponse,if Yes

Write off recommendations will be prepared for provider
(viii)

Payment will be posted after verifying claim`s processing informations
(ix)

Patient Responsibility
(x)

Analysis

(I)(II)(III)(IV)(V)
Action:Review
Reason:Duplicate
Group:Denials

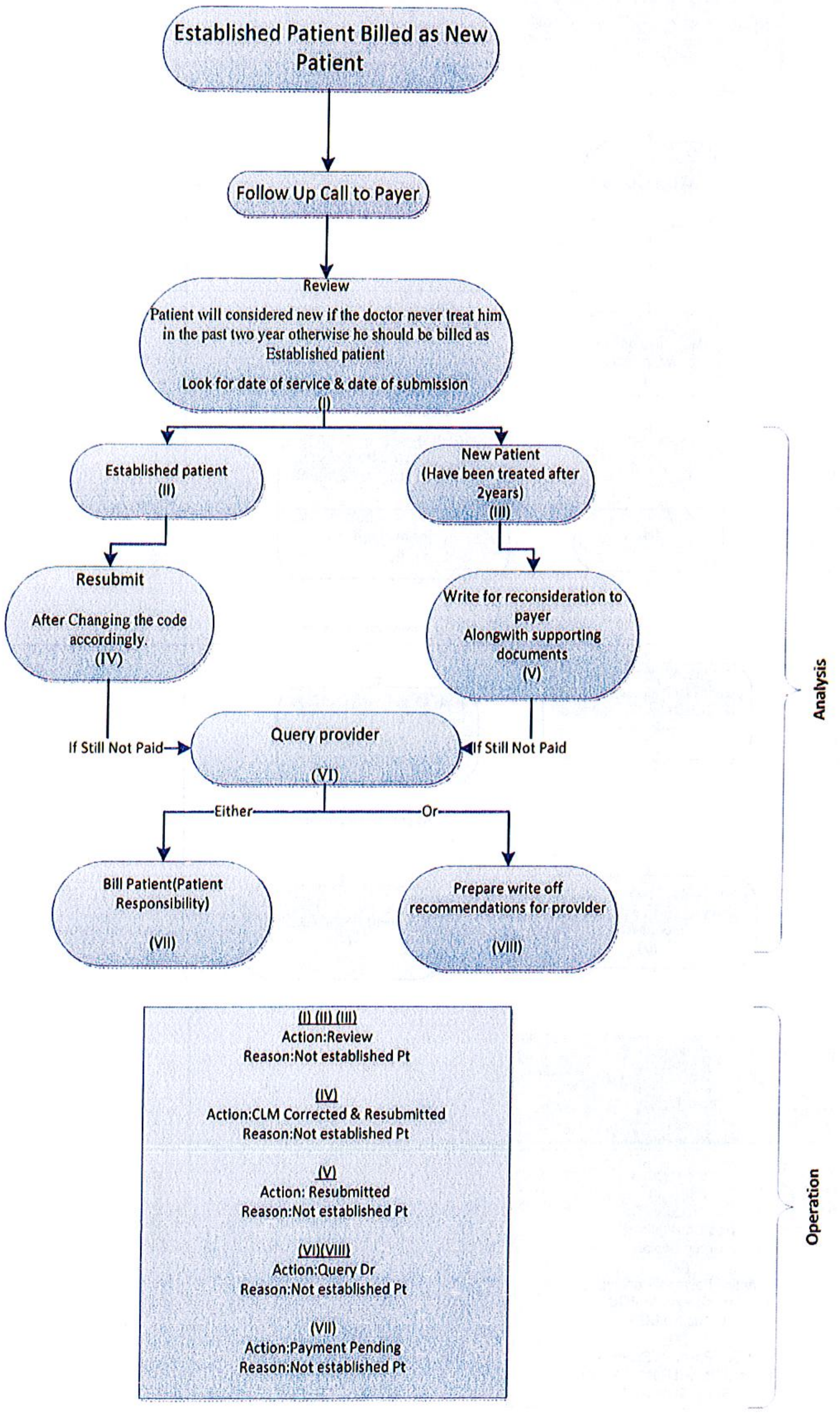
(VI)
Action:Call Required
Reason:Duplicate
Group:Denials

(VII)(VIII)
Action:Query Dr
Reason:Duplicate
Group:Denials

(IX)
Action:Payment Pending
Reason:Missing EOB
Group:No EOB

(X)
Action:Payment Pending
Reason:Patient Responsibility
Group:Statement

Operation


Established Patient Billed as New Patient
Follow Up Call to Payer
Review
Patient will considered new if the doctor never treat him in the past two year otherwise he should be billed as Established patient
Look for date of service & date of submission
(I)
Established patient
(II)
New Patient
(Have been treated after 2years)
(III)
Resubmit
After Changing the code accordingly.
(IV)
Write for reconsideration to payer
Alongwith supporting documents
(V)
If Still Not Paid
Query provider
(VI)
If Still Not Paid
Either
Or
Bill Patient(Patient Responsibility)
(VII)
Prepare write off recommendations for provider
(VIII)
Analysis
Operation

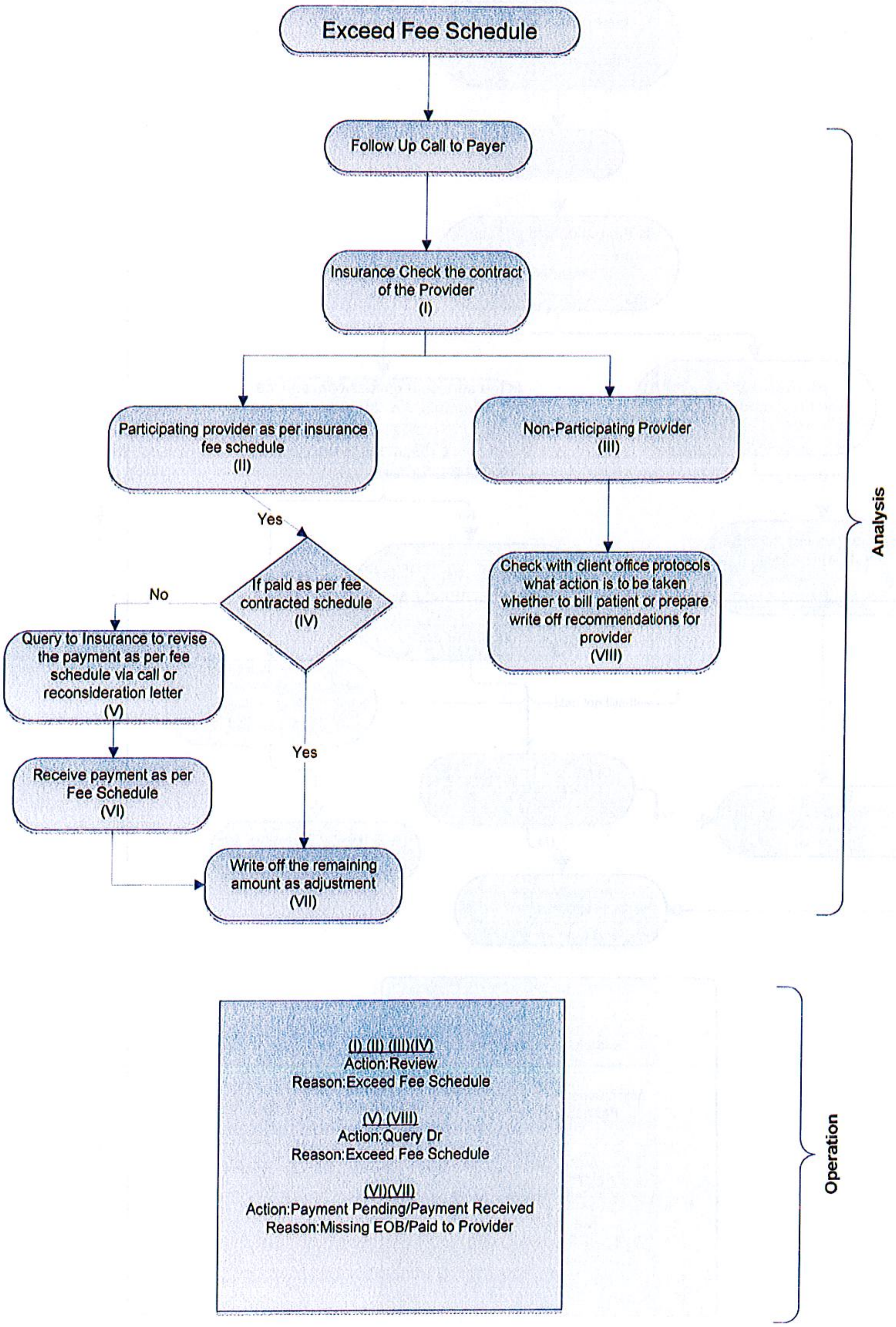
(I) (II) (III)
Action:Review
Reason:Not established Pt

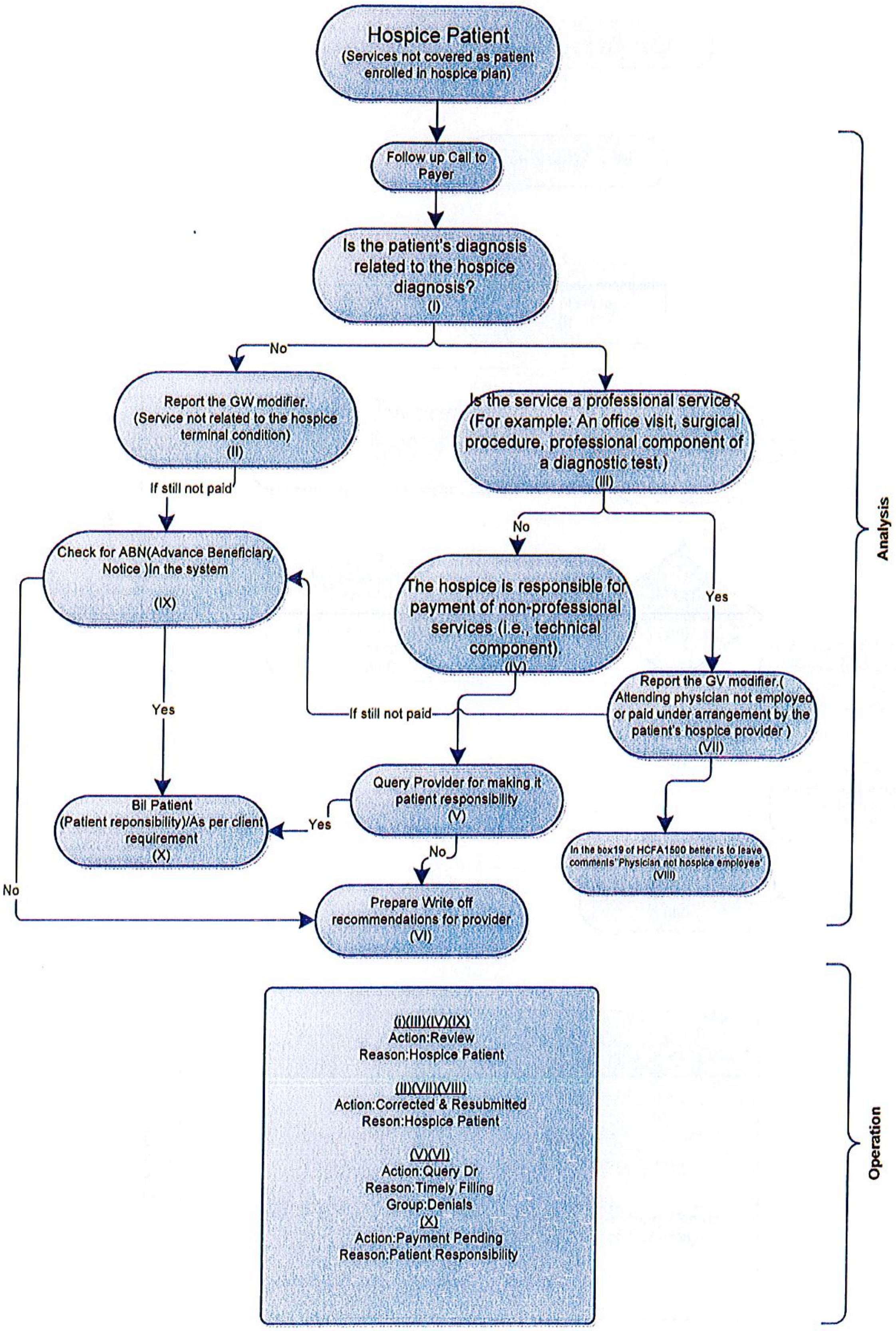
(IV)
Action:CLM Corrected & Resubmitted
Reason:Not established Pt

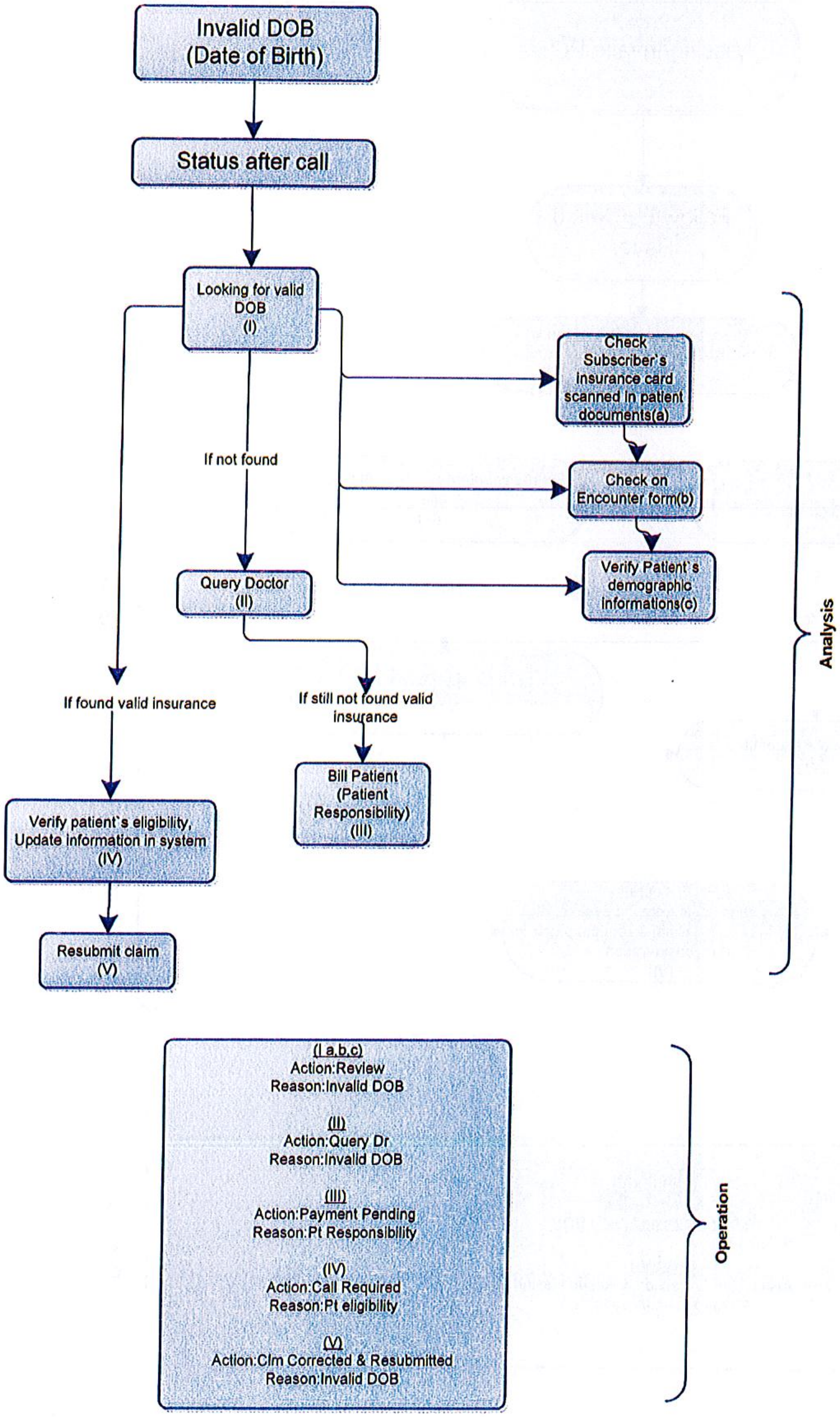
(V)
Action: Resubmitted
Reason:Not established Pt

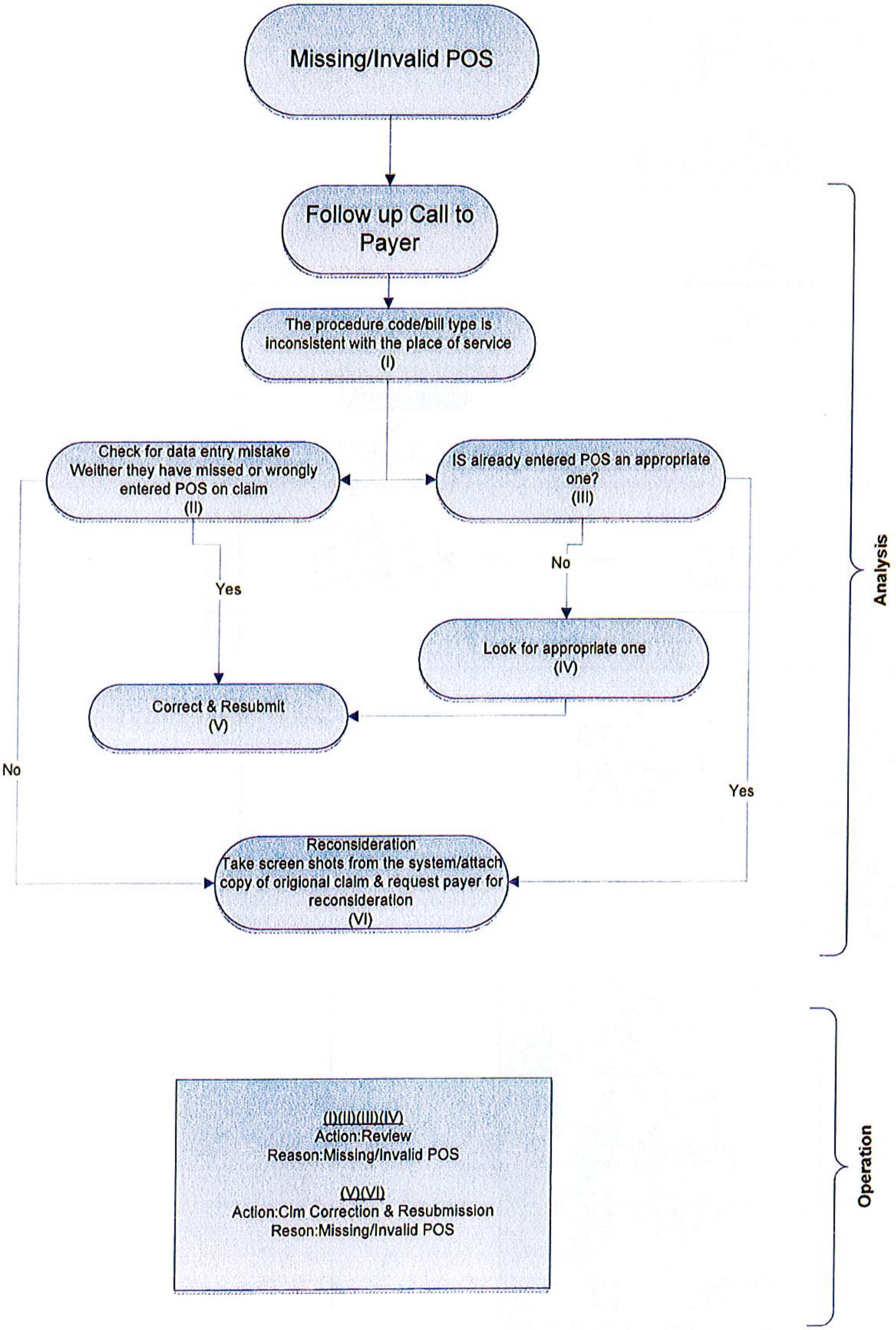
(VI)(VIII)
Action:Query Dr
Reason:Not established Pt

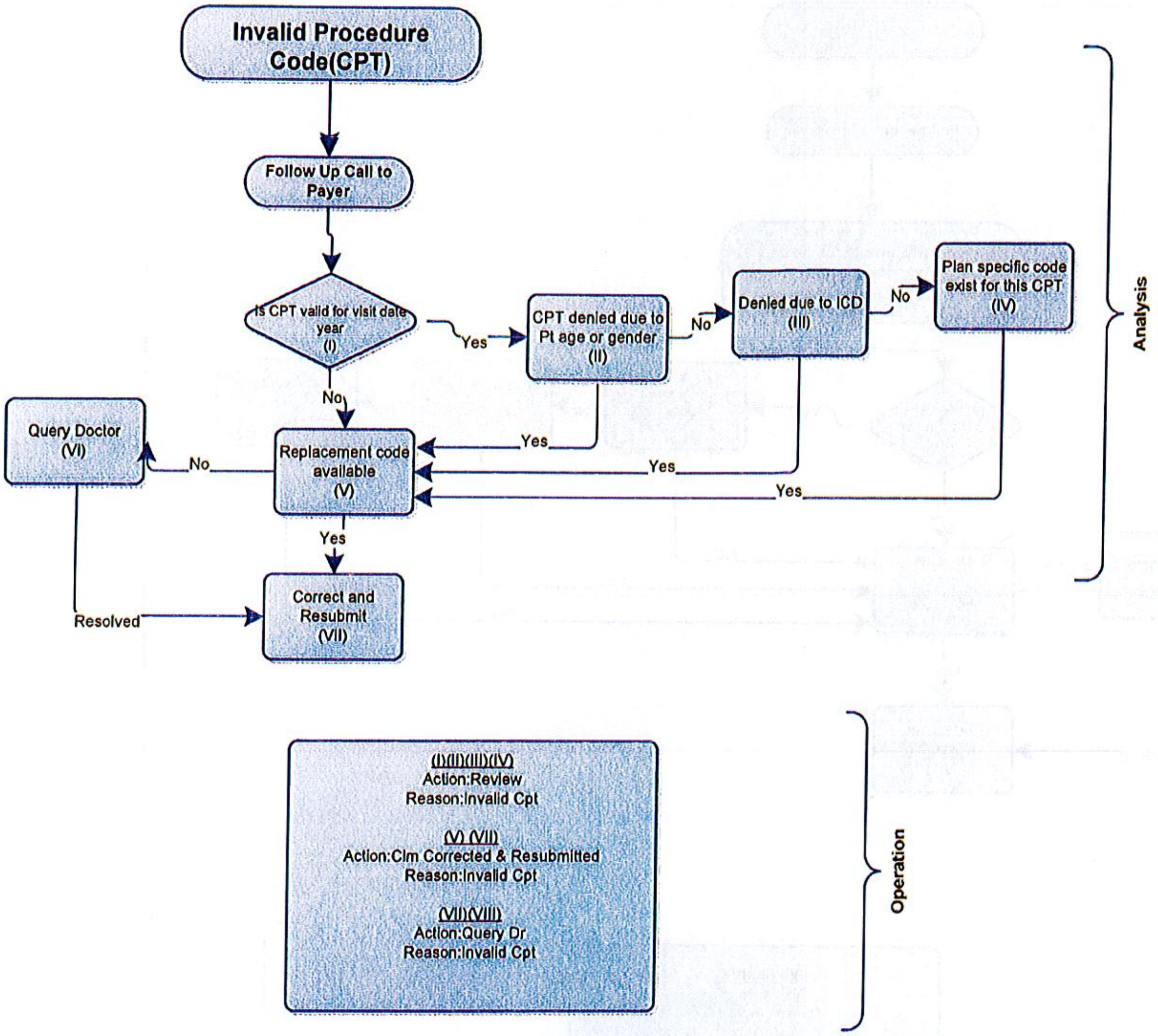
(VII)
Action:Payment Pending
Reason:Not established Pt

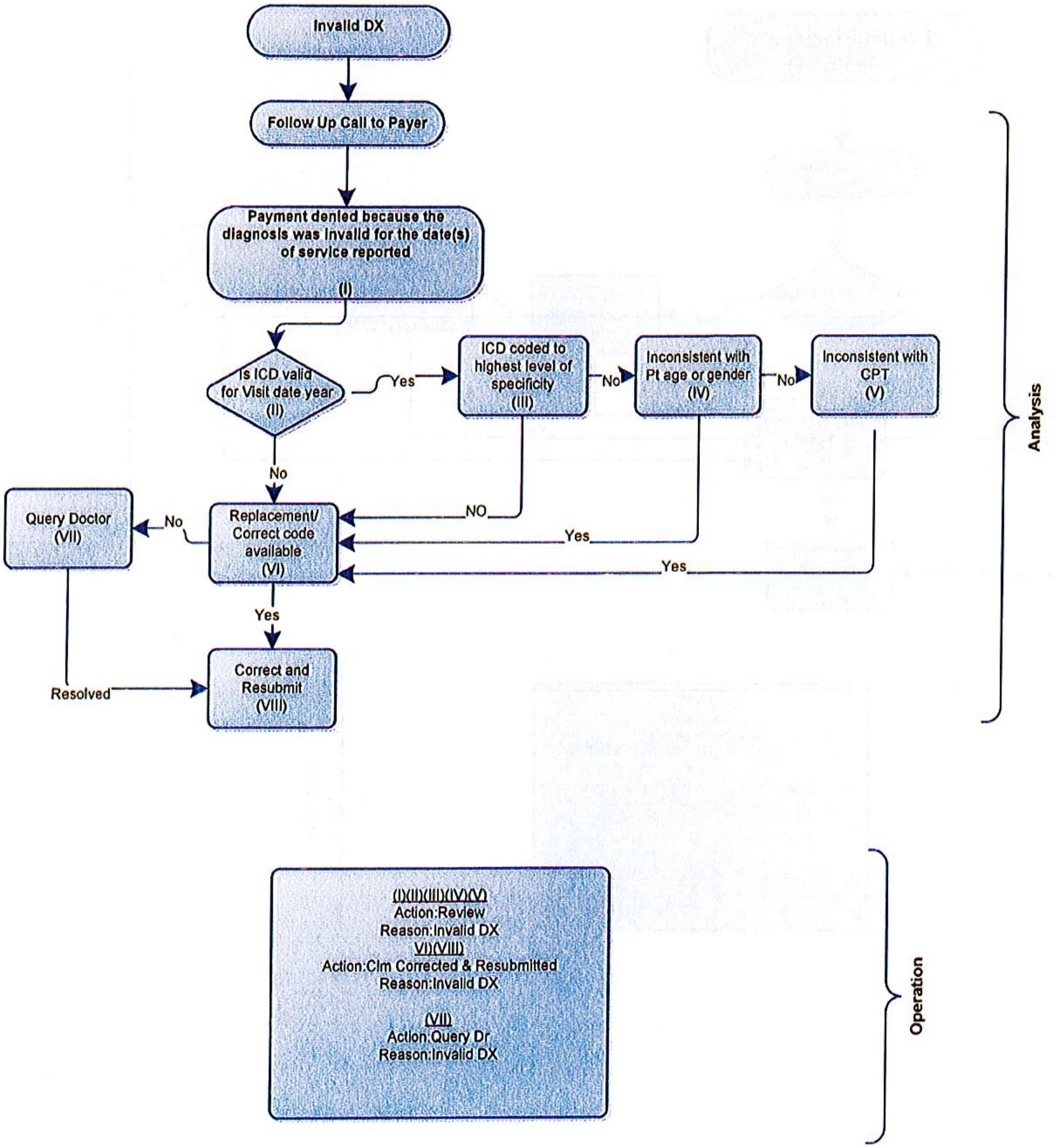

Exceed Fee Schedule
Follow Up Call to Payer
Insurance Check the contract of the Provider (I)
Participating provider as per insurance fee schedule (II)
Non-Participating Provider (III)
Yes
If paid as per fee contracted schedule (IV)
No
Query to Insurance to revise the payment as per fee schedule via call or reconsideration letter (V)
Receive payment as per Fee Schedule (VI)
Yes
Write off the remaining amount as adjustment (VII)
Check with client office protocols what action is to be taken whether to bill patient or prepare write off recommendations for provider (VIII)
Analysis
(I) (II) (III)(IV)
Action:Review
Reason:Exceed Fee Schedule
(V) (VIII)
Action:Query Dr
Reason:Exceed Fee Schedule
(VI)(VII)
Action:Payment Pending/Payment Received
Reason:Missing EOB/Paid to Provider
Operation

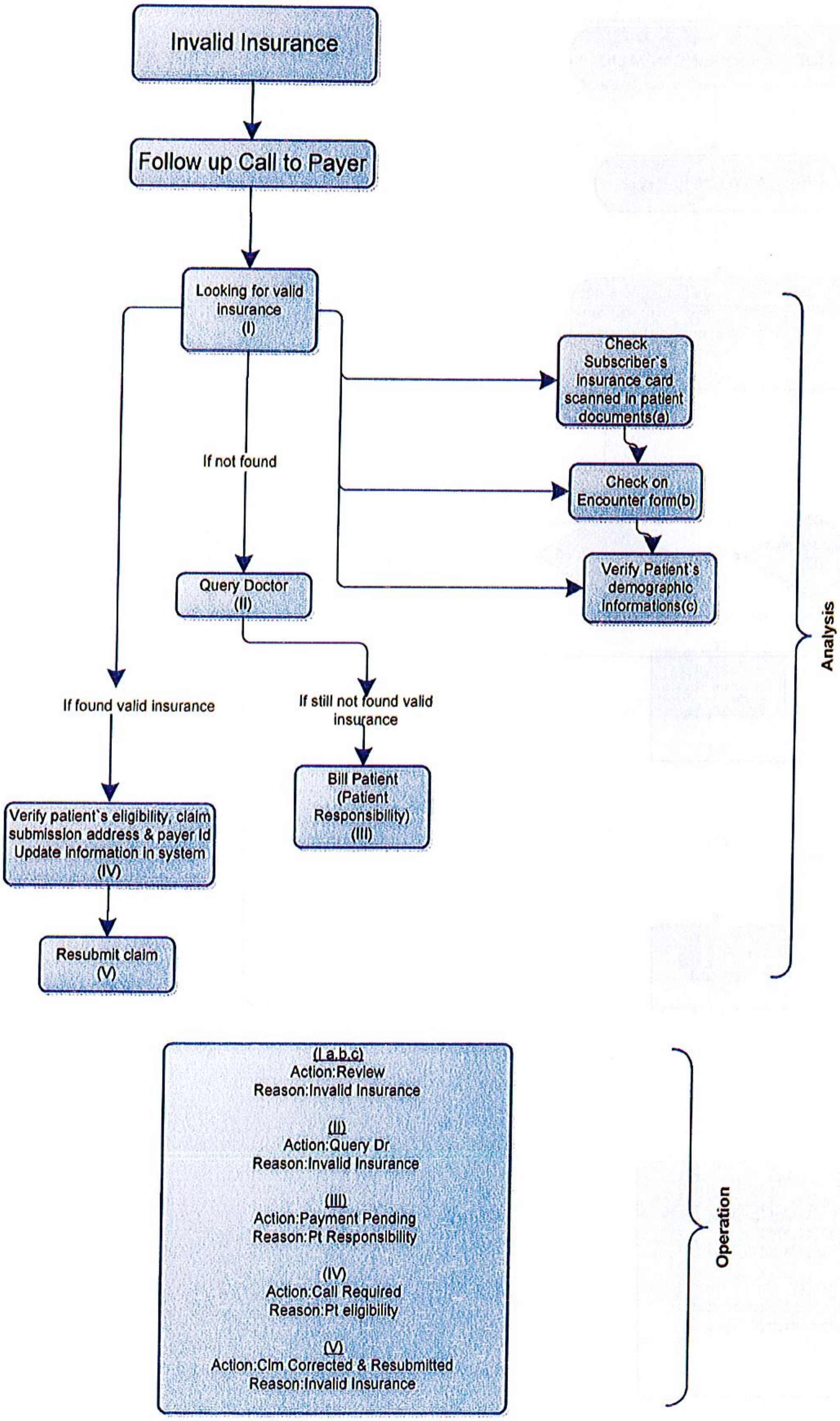

Hospice Patient
(Services not covered as patient enrolled in hospice plan)
Follow up Call to Payer
Is the patient's diagnosis related to the hospice diagnosis?
(I)
No
Report the GW modifier.
(Service not related to the hospice terminal condition)
(II)
Is the service a professional service?
(For example: An office visit, surgical procedure, professional component of a diagnostic test.)
(III)
If still not paid
Check for ABN(Advance Beneficiary Notice)In the system
(IX)
No
The hospice is responsible for payment of non-professional services (i.e., technical component).
(IV)
Yes
Report the GV modifier.(Attending physician not employed or paid under arrangement by the patient's hospice provider)
(VII)
If still not paid
Yes
Query Provider for making it patient responsibility
(V)
Bil Patient
(Patient reponsibility)/As per client requirement
(X)
Yes
No
No
In the box19 of HCFA1500 better is to leave comments"Physician not hospice employee"
(VIII)
Prepare Write off recommendations for provider
(VI)
Analysis
(I)(III)(IV)(IX)
Action:Review
Reason:Hospice Patient
(II)(VII)(VIII)
Action:Corrected & Resubmitted
Reson:Hospice Patient
(V)(VI)
Action:Query Dr
Reason:Timely Filling
Group:Denials
(X)
Action:Payment Pending
Reason:Patient Responsibility
Operation

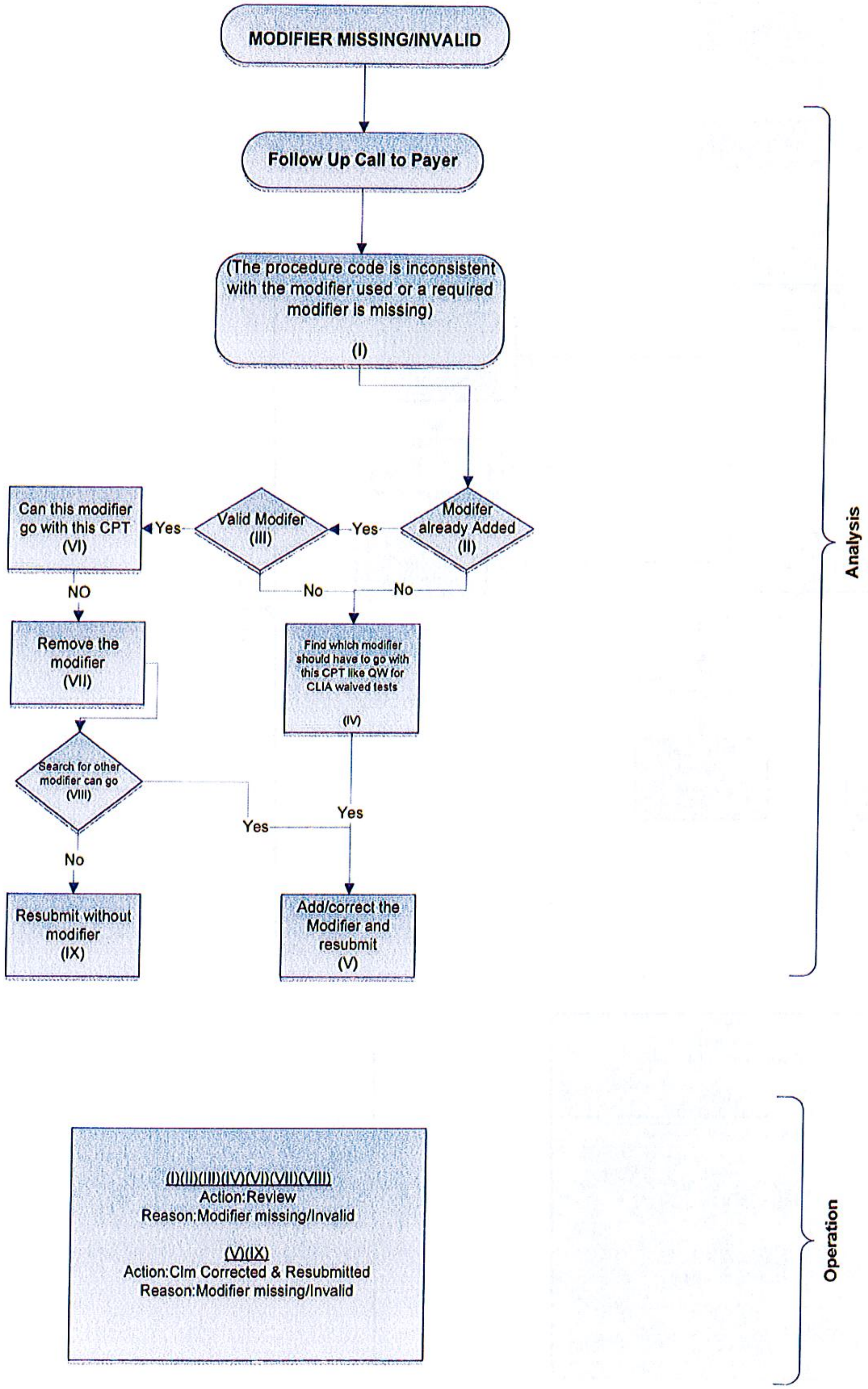

Invalid DOB (Date of Birth)
Status after call
Looking for valid DOB (I)
Check Subscriber's insurance card scanned in patient documents(a)
Check on Encounter form(b)
Verify Patient's demographic informations(c)
If not found
Query Doctor (II)
If found valid insurance
If still not found valid insurance
Bill Patient (Patient Responsibility) (III)
Verify patient's eligibility, Update information in system (IV)
Resubmit claim (V)
Analysis
(I a,b,c)
Action:Review
Reason:Invalid DOB
(II)
Action:Query Dr
Reason:Invalid DOB
(III)
Action:Payment Pending
Reason:Pt Responsibility
(IV)
Action:Call Required
Reason:Pt eligibility
(V)
Action:Clm Corrected & Resubmitted
Reason:Invalid DOB
Operation

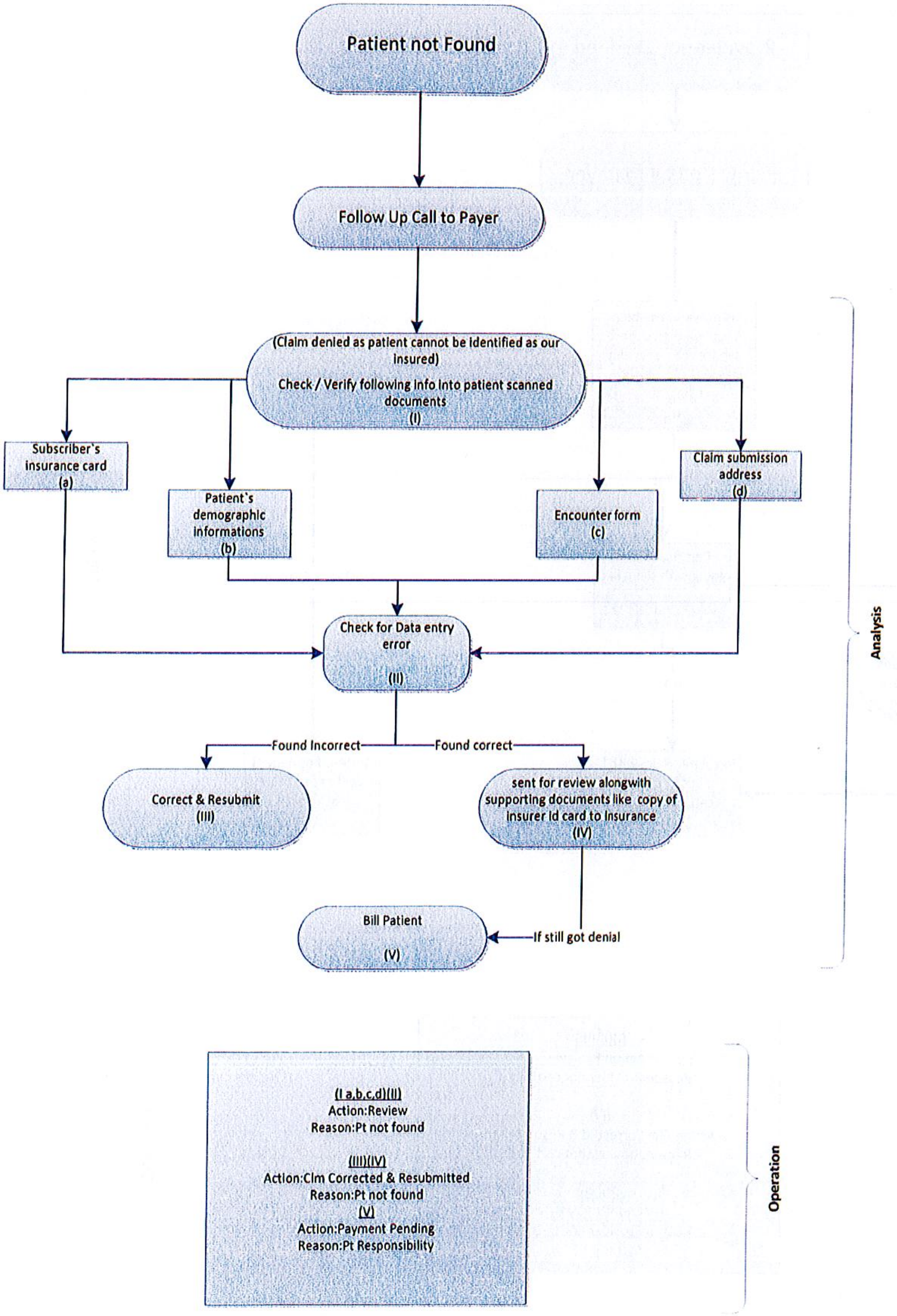

Missing/Invalid POS
Follow up Call to Payer
The procedure code/bill type is inconsistent with the place of service (I)
Check for data entry mistake Weither they have missed or wrongly entered POS on claim (II)
IS already entered POS an appropriate one? (III)
No
Yes
Look for appropriate one (IV)
Correct & Resubmit (V)
No
Yes
Reconsideration Take screen shots from the system/attach copy of origional claim & request payer for reconsideration (VI)
Analysis
(I)(II)(III)(IV)
Action:Review
Reason:Missing/Invalid POS
(V)(VI)
Action:Clm Correction & Resubmission
Reson:Missing/Invalid POS
Operation

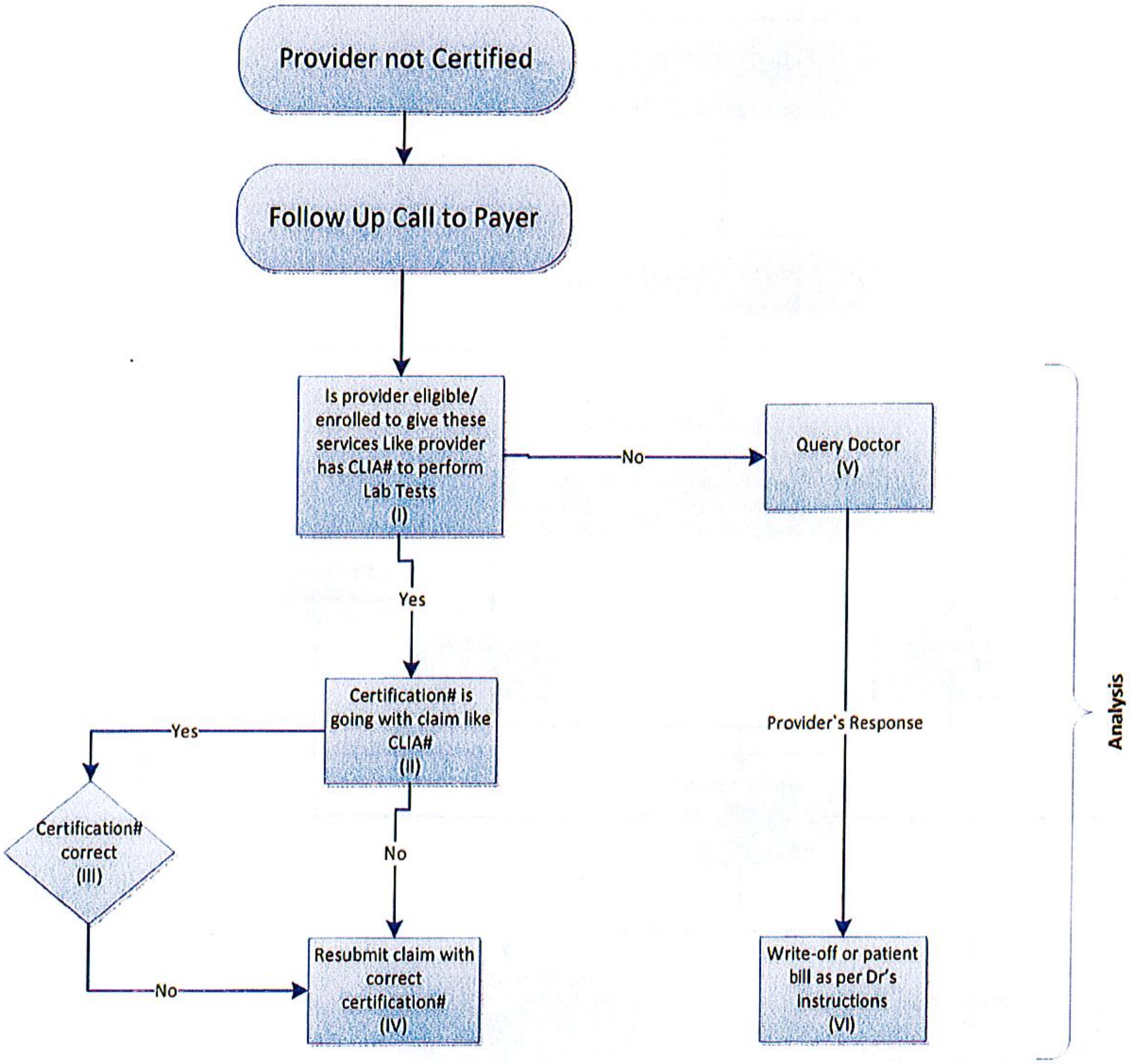

Invalid Procedure Code(CPT)
Follow Up Call to Payer
Is CPT valid for visit date year (I)
Yes
CPT denied due to Pt age or gender (II)
No
Denied due to ICD (III)
No
Plan specific code exist for this CPT (IV)
No
Query Doctor (VI)
No
Replacement code available (V)
Yes
Yes
Yes
Yes
Resolved
Correct and Resubmit (VII)
Analysis
(I)(II)(III)(IV)
Action:Review
Reason:Invalid Cpt
(V) (VII)
Action:Clm Corrected & Resubmitted
Reason:Invalid Cpt
(VI)(VIII)
Action:Query Dr
Reason:Invalid Cpt
Operation


Invalid DX
Follow Up Call to Payer
Payment denied because the diagnosis was invalid for the date(s) of service reported
(I)
Is ICD valid for Visit date year
(II)
Yes
ICD coded to highest level of specificity
(III)
No
Inconsistent with Pt age or gender
(IV)
No
Inconsistent with CPT
(V)
No
NO
Yes
Yes
Replacement/ Correct code available
(VI)
No
Query Doctor
(VII)
Yes
Correct and Resubmit
(VIII)
Resolved
Analysis
(I)(II)(III)(IV)(V)
Action:Review
Reason:Invalid DX
VI)(VIII)
Action:Clm Corrected & Resubmitted
Reason:Invalid DX
(VII)
Action:Query Dr
Reason:Invalid DX
Operation


Invalid Insurance
Follow up Call to Payer
Looking for valid insurance (I)
Check Subscriber`s insurance card scanned in patient documents(a)
Check on Encounter form(b)
Verify Patient`s demographic informations(c)
If not found
Query Doctor (II)
If found valid insurance
If still not found valid insurance
Bill Patient (Patient Responsibility) (III)
Verify patient`s eligibility, claim submission address & payer Id Update information in system (IV)
Resubmit claim (V)
Analysis
(I a,b,c)
Action:Review
Reason:Invalid Insurance
(II)
Action:Query Dr
Reason:Invalid Insurance
(III)
Action:Payment Pending
Reason:Pt Responsibility
(IV)
Action:Call Required
Reason:Pt eligibility
(V)
Action:Clm Corrected & Resubmitted
Reason:Invalid Insurance
Operation


MODIFIER MISSING/INVALID
Follow Up Call to Payer
(The procedure code is inconsistent with the modifier used or a required modifier is missing)
(I)
Modifer already Added
(II)
Yes
Valid Modifer
(III)
Yes
Can this modifier go with this CPT
(VI)
No
No
NO
Remove the modifier
(VII)
Find which modifier should have to go with this CPT like QW for CLIA waived tests
(IV)
Search for other modifier can go
(VIII)
Yes
Yes
No
Resubmit without modifier
(IX)
Add/correct the Modifier and resubmit
(V)
Analysis
(I)(II)(III)(IV)(VI)(VII)(VIII)
Action:Review
Reason:Modifier missing/Invalid
(V)(IX)
Action:Clm Corrected & Resubmitted
Reason:Modifier missing/Invalid
Operation


Patient not Found
Follow Up Call to Payer
(Claim denied as patient cannot be identified as our insured)
Check / Verify following info into patient scanned documents
(I)
Subscriber's insurance card
(a)
Patient's demographic informations
(b)
Encounter form
(c)
Claim submission address
(d)
Check for Data entry error
(II)
Found Incorrect
Found correct
Correct & Resubmit
(III)
sent for review alongwith supporting documents like copy of insurer id card to Insurance
(IV)
If still got denial
Bill Patient
(V)
Analysis
(I a,b,c,d)(II)
Action:Review
Reason:Pt not found
(III)(IV)
Action:Clm Corrected & Resubmitted
Reason:Pt not found
(V)
Action:Payment Pending
Reason:Pt Responsibility
Operation

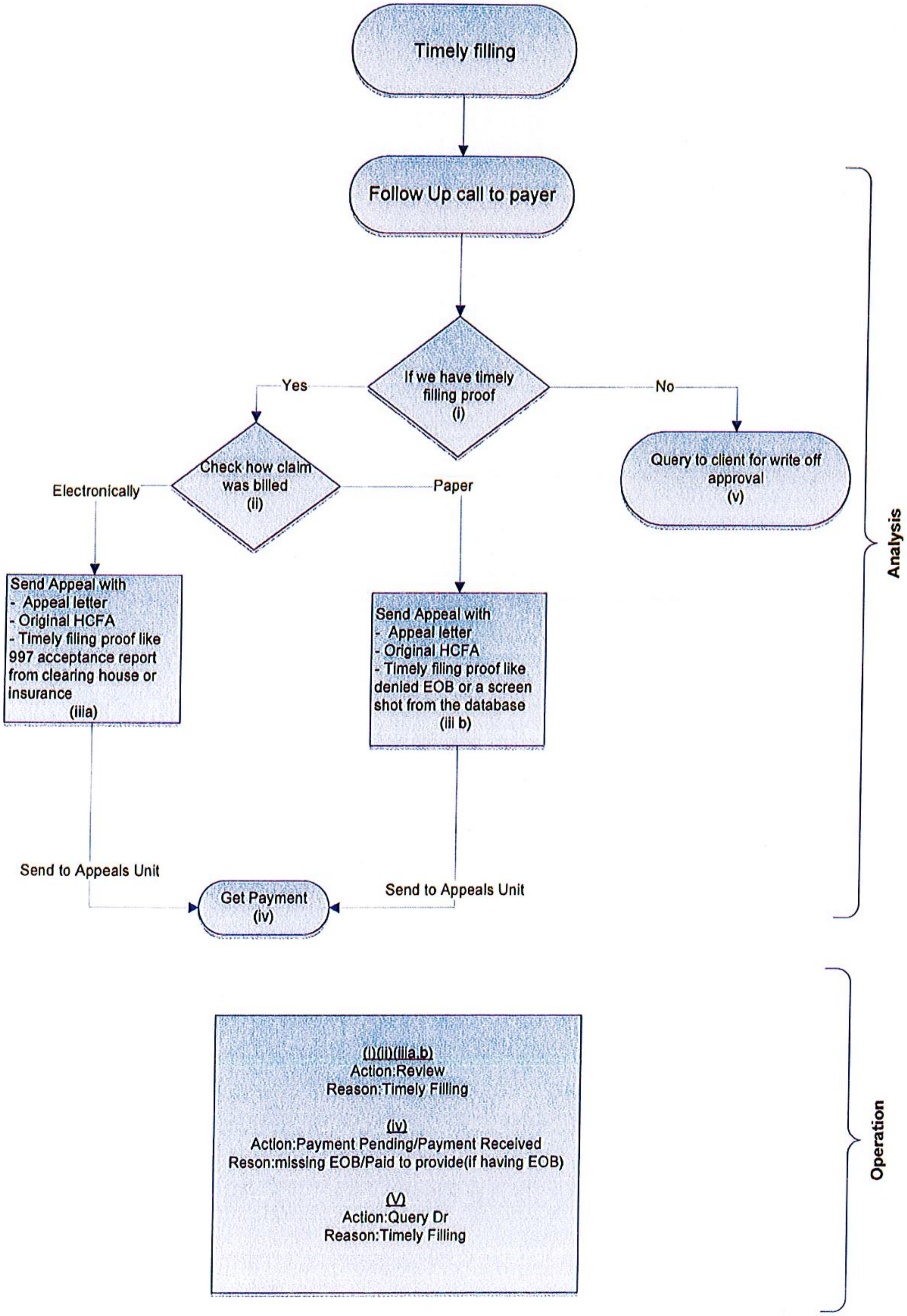

Provider not Certified
Follow Up Call to Payer
Is provider eligible/ enrolled to give these services Like provider has CLIA# to perform Lab Tests (I)
No
Query Doctor (V)
Yes
Certification# is going with claim like CLIA# (II)
Yes
Certification# correct (III)
No
No
Resubmit claim with correct certification# (IV)
Provider's Response
Write-off or patient bill as per Dr's instructions (VI)
Analysis

(I)(II)(III)
Action:Review
Reason:Provider not certified

(IV)
Action:Clm Corrected & Resubmitted
Reason:Provider not certified

(V)(VI)
Action:Query Dr
Reason:Provider not certified

Operation


Timely filling
Follow Up call to payer
If we have timely filling proof (i)
Yes
No
Query to client for write off approval (v)
Check how claim was billed (ii)
Electronically
Paper
Send Appeal with
- Appeal letter
- Original HCFA
- Timely filing proof like 997 acceptance report from clearing house or insurance
(iiia)
Send Appeal with
- Appeal letter
- Original HCFA
- Timely filing proof like denied EOB or a screen shot from the database
(iii b)
Send to Appeals Unit
Send to Appeals Unit
Get Payment (iv)
Analysis
(i)(ii)(iiia,b)
Action:Review
Reason:Timely Filling
(iv)
Action:Payment Pending/Payment Received
Reson:missing EOB/Paid to provide(if having EOB)
(V)
Action:Query Dr
Reason:Timely Filling
Operation