FILED
2009 JUL 13 PM 3:25
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES
BY

GARY DUKARICH, CA Bar No. 188561
E-mail: gsd@cph.com
CHRISTIE, PARKER & HALE, LLP
3501 Jamboree Road. Suite 6000
Newport Beach, California 92660-2960
Telephone: (949) 476-0757
Facsimile: (949) 476-8640

Attorneys for Plaintiff,
Medversant Technologies, L.L.C.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

MEDVERSANT TECHNOLOGIES, L.L.C., Plaintiff, vs. MORRISEY ASSOCIATES, INC., Defendant.	Case No. CV09-05031 MMM (RCx) **COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

For its complaint against Defendant Morrisey Associates, Inc. ("Morrisey"), Plaintiff Medversant Technologies, L.L.C. ("Medversant") alleges as follows:

JURISDICTION

1. This is an action for patent infringement pursuant to 35 U.S.C. Section 271. This Court has jurisdiction pursuant to 28 U.S.C. Section 1338(a).

2. Venue is proper under 28 U.S.C. Sections 1391(b)(2).

PARTIES

3. Plaintiff Medversant is a limited liability company organized and existing under the laws of the State of California, having a principal place of business at Two California Plaza, 350 South Grand Avenue, Suite 3070, Los Angeles, California 90071.

4. Plaintiff is informed and believes, and thereon alleges that Defendant Morrissey is a U.S. corporation, having a principal place of business at 222 South Riverside Plaza, Suite 1850, Chicago, Illinois 60606.

FACTUAL BACKGROUND

5. Medversant is a developer and distributor of web-based credentialing systems for automatically, electronically managing practitioner credentialing information.

6. On December 11, 2002, Medversant filed a U.S. patent application directed to its automated system of credentialing management. U.S. Patent Number 7,529,682 (the "'682 Patent"), entitled "Electronic Credentials Verification and Management System," issued on May 5, 2009 and was assigned to Medversant. A true and correct copy of the '682 Patent is attached hereto as Exhibit A.

7. Morrisey has sold and offered for sale in this District and elsewhere, and continues to sell and offer for sale in this District and elsewhere, without the consent or authorization of Medversant, one or more products or systems directed to automated electronic credentials verification, including without limitation a product known as "MSO for the Web" or "MSOW", that are covered by one or more claims of the '682 Patent (the "Infringing Products").

FIRST CLAIM FOR RELIEF

Patent Infringement

8. Medversant hereby repeats and realleges paragraphs 1 through 7 hereinabove as though fully set forth herein.

9. Morrisey, by itself or in concert with others, has made, used, sold or offered to sell, and continues to make, use, sell or offer to sell, in this District and elsewhere in the United States, the Infringing Products which infringe the '682 Patent.

10. The aforesaid acts of Morrisey are without right, license, or authorization from Medversant.

11. By its aforesaid acts, Morrisey has infringed the '682 Patent, entitling Medversant to relief pursuant to 35 U.S.C. Section 271.

12. Morrisey has had actual or constructive notice of the existence of the '682 Patent, and despite such notice has continued to engage in acts of infringement.

13. Because of Morrisey's acts complained of herein, Medversant has been actually damaged and irreparably harmed and Morrisey has been unjustly enriched, to an extent not presently ascertained, which damage, harm and enrichment will continue until enjoined by order of this Court.

14. Morrisey's infringement of the '682 patent is and has been willful and Medversant is entitled to enhanced damages against Morrisey.

15. This is an exceptional case and Medversant is entitled to an award of its attorneys' fees.

PRAYER

WHEREFORE, Plaintiff Medversant demands judgment against Defendant Morrisey as follows:

1. Adjudging and decreeing that Morrisey has committed acts of patent infringement by its manufacture, use, sale, and offer for sale of the Infringing Products;

2. For a temporary and permanent injunction prohibiting Morrisey and its officers, agents, servants, employees and attorneys, and other persons in active concert or participation with them, from further infringing the '682 Patent, and requiring Morrisey to deliver up to Medversant for destruction any and all Infringing Products in Morrisey's possession, custody or control, along with any items of manufacture, the sole purpose of which is to manufacture such Infringing Products, as well as any promotional literature and packaging which displays or promotes such Infringing Products.

3. For patent infringement damages in an amount not less than a reasonable royalty, and for those damages to be trebled, pursuant to 35 U.S.C. Section 284;

4. For prejudgment interest;

5. For all of Medversant's costs of this Action, including attorneys' fees; and

6. For such other or further relief as the Court may deem just and proper.

DATED: July 13, 2009

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____
Gary Dukarich

Attorneys for Plaintiff,
MEDVERSANT TECHNOLGIES, L.L.C.

DEMAND FOR JURY TRIAL

Plaintiff Medversant Technologies, L.L.C., pursuant to Federal Rule of Civil Procedure 38, hereby demands a trial by jury of all issues so triable.

DATED: July 13, 2009

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____
Gary Dukarich

Attorneys for Plaintiff,
MEDVERSANT TECHNOLGIES, L.L.C.

KMG IRV1117506.1-*-07/13/09 11:04 AM

EXHIBIT A

US007529682B2

(12) **United States Patent**
Geller et al.

(10) **Patent No.: US 7,529,682 B2**
(45) **Date of Patent: May 5, 2009**

(54) **ELECTRONIC CREDENTIALS VERIFICATION AND MANAGEMENT SYSTEM**

(75) Inventors: **Marilyn Grunzweig Geller**, West Hills, CA (US); **Jiehong Tang**, Hacienda Heights, CA (US); **Matthew J. Haddad**, Marina del Rey, CA (US)

(73) Assignee: **Medversant Technologies, LLC**, Los Angeles, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1091 days.

(21) Appl. No.: **10/316,821**

(22) Filed: **Dec. 11, 2002**

(65) **Prior Publication Data**

US 2004/0117617 A1 Jun. 17, 2004

(51) **Int. Cl.**
G06Q 99/00 (2006.01)

(52) **U.S. Cl.** **705/1**

(58) **Field of Classification Search** 705/1
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,553,206	A		11/1985	Smutek et al.
4,878,175	A		10/1989	Norden-Paul et al.
5,070,452	A		12/1991	Doyle, Jr. et al.
5,225,976	A		7/1993	Tawil
5,235,702	A		8/1993	Miller
5,301,105	A		4/1994	Cummings, Jr.
5,325,293	A		6/1994	Dorne
5,359,509	A		10/1994	Little et al.
5,557,514	A	*	9/1996	Seare et al. 705/2
5,706,441	A		1/1998	Lockwood
5,778,345	A		7/1998	McCartney
5,812,984	A		9/1998	Goltra
6,035,276	A	*	3/2000	Newman et al. 705/2
6,144,959	A		11/2000	Anderson et al.
7,263,491	B1	*	8/2007	Geldermann et al. 705/1
2002/0065758	A1	*	5/2002	Henley 705/37
2003/0236682	A1	*	12/2003	Heyer 705/2

OTHER PUBLICATIONS

Computer Security update; "Medquist selects Presideo for Security Featuring Verisign."; Dec. 1, 2000.*

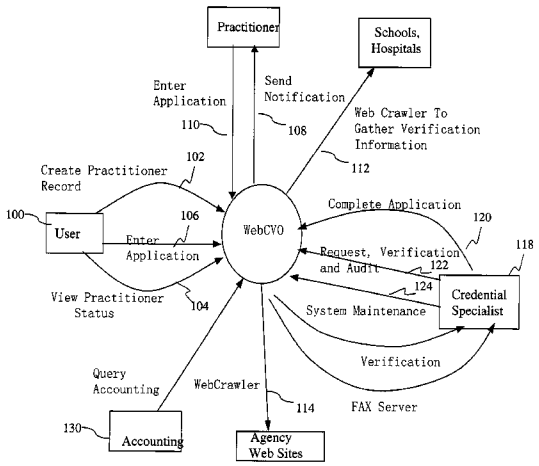
(Continued)

Primary Examiner—Jonathan Ouellette
(74) *Attorney, Agent, or Firm*—Christie, Parker & Hale, LLP.

(57) **ABSTRACT**

A credentials record system that creates and maintains all personnel data electronically is disclosed. The system captures personnel background data, such as license information, education and training, work experience, performance data and electronic signature at the time of entry using graphical user interfaces through a network. For example, computers with Internet connections may be used by authorized personnel to access, analyze, update and electronically annotate data even while other users are using the same record. An exemplary system may archive historical data is archived to create and record an audit trail of changes by the users. The system permits instant, sophisticated analysis of background data to identify relationships among the data, including archived data. Moreover, the system includes the capability to access reference databases for consultation regarding verification of data for accuracy on a continuous basis. The system also provides for an automated auditing process to ensure data integrity. The system may also include the capability to incorporate legacy data, such as paper files and mainframe data, for each personnel record.

36 Claims, 10 Drawing Sheets



OTHER PUBLICATIONS

PR Newswire; "CompHealth Credentialing Services Certified by National Committee for Quality Assurance" Feb. 22, 2001.*
PR Newswire; "CREDENT Receives Highest Certification from the National Committee for Quality Assurance"; Oct. 29, 2001.*
Chicago Sun-Times; "Doctor's credentials need Checking"; Howard Wolinsky; Feb. 21, 1988.*
"Will your compliance plan pass the effectiveness test?"; Lawrence A Foge; Healthcare Financial Mangement; Apr. 2000.*
PCT International Search Report dated Sep. 29, 2004, Application No. PCT/US03/39603.
Hernandez, Arthur M., "Trends in Health Care Practitioner Credentialing", Journal of Health Care Finance, Spring 1998, pp. 66-70, vol. 24:3, Aspen Publishers, Inc., U.S.
Nelson, Patricia, "Measuring the Quality of Chiropractic Alternative Care in a Managed Care Environment", Topics in Health Information Management, May 1998, pp. 39-45, vol. 18:4, Aspen Publishers, Inc., U.S.
Ruth, Linda C. et al., "Assessing Health Plan Quality", Benefits Quarterly, 1995, pp. 32-36, Second Quarter, U.S.
"MedQuist Selects Presideo for Security Featuring Versign", Worldwide Videotex, Dec. 1, 2000, vol. 1, Issue 12, Boynton Beach.
"CompHealth Credentialing Services Certified by the National Committee for Quality Assurance", PR Newswire, Feb. 22, 2001, p. 1, New York.
"CREDENT Receives Highest Certification from the National Committee for Quality Assurance", PR Newswire, Oct. 29, 2001, p. 1, New York.
"Doctors' Credentials Need Checking", Chicago Sun-Times, Feb. 21, 1988, p. 14, Chicago.

* cited by examiner

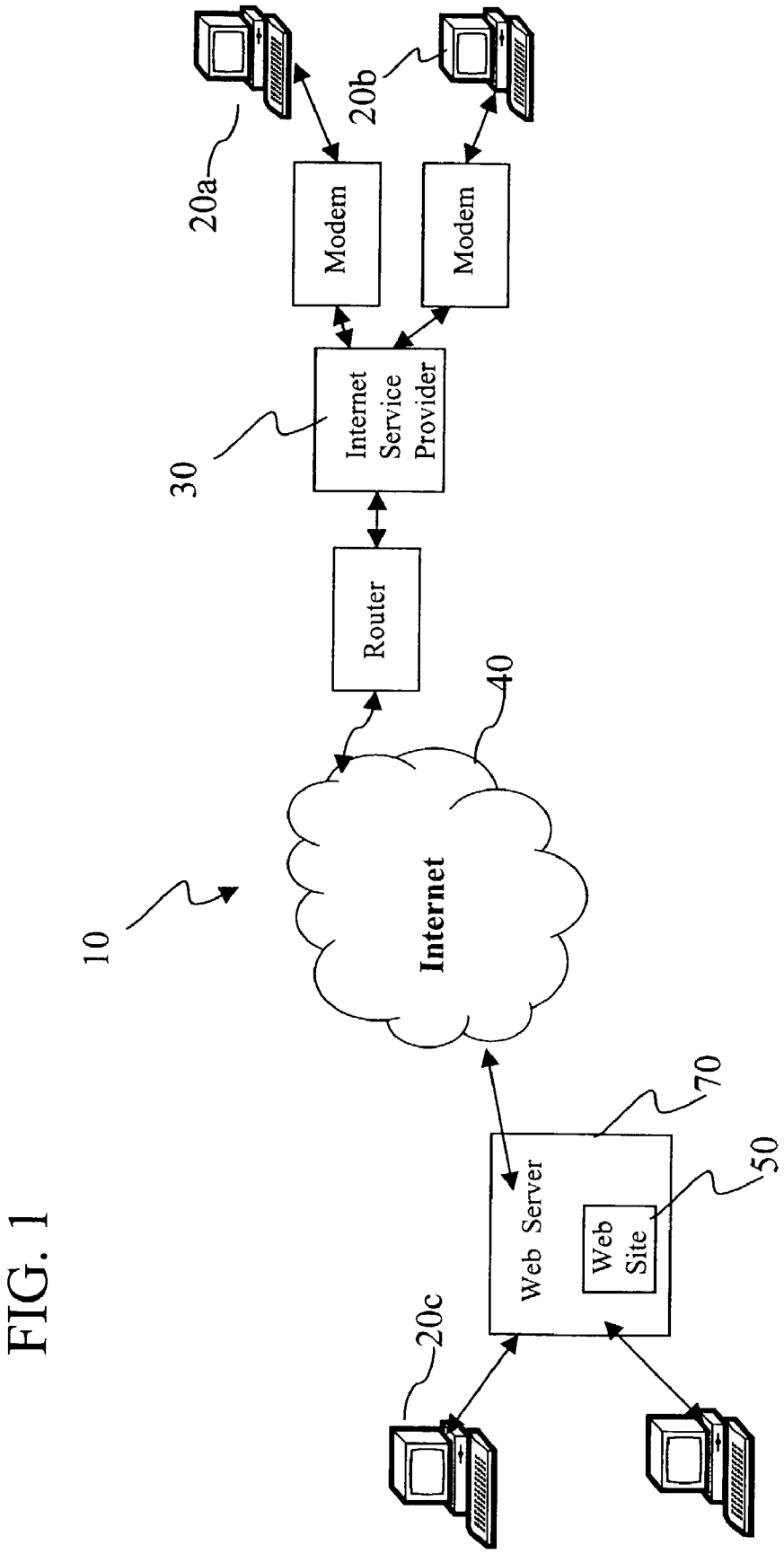

20a
20b
Modem
Modem
Internet Service Provider
30
Router
40
Internet
10
70
Web Server
Web Site
50
20c

FIG. 1

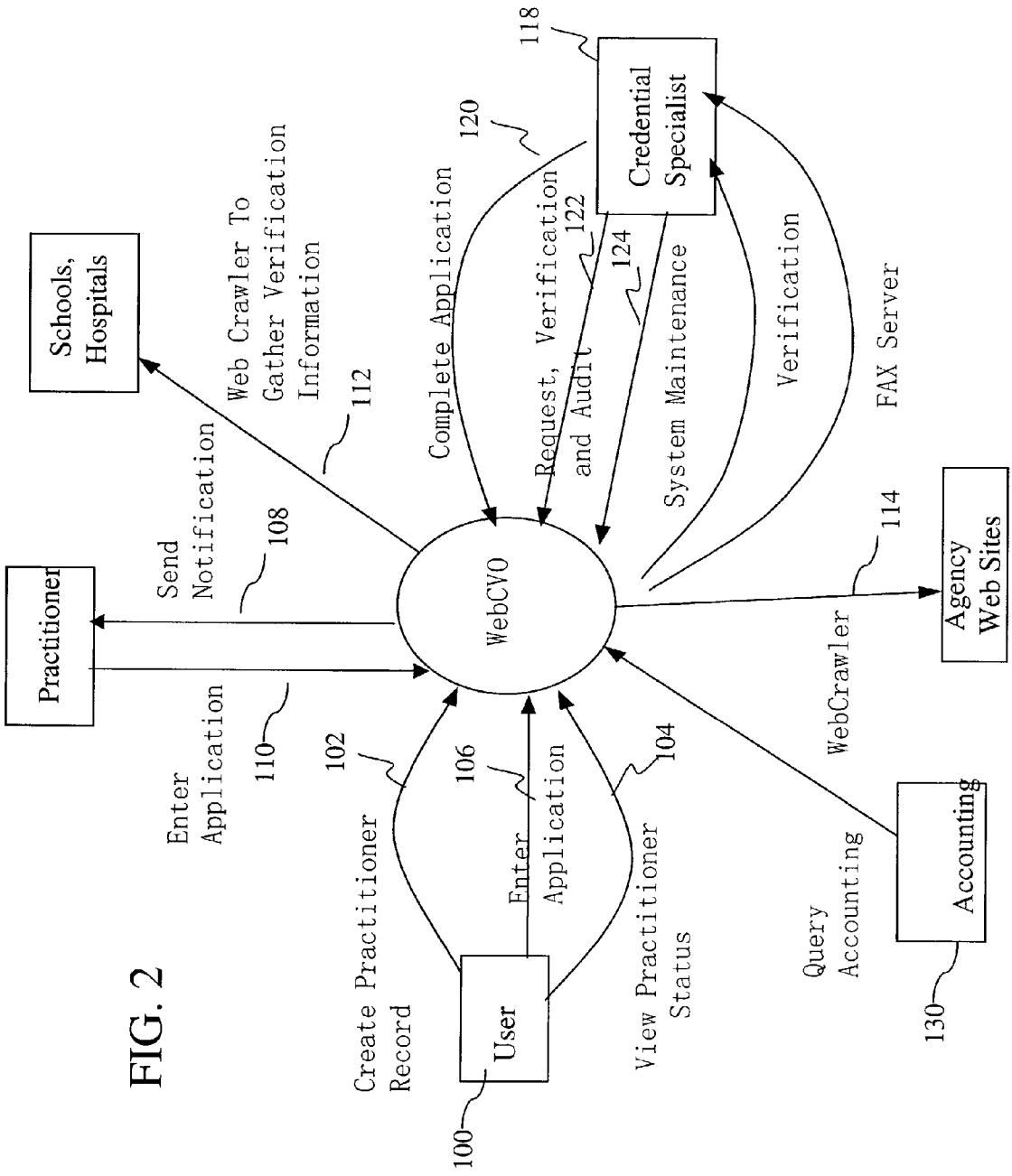

Schools, Hospitals
Practitioner
User
WebCVO
Credential Specialist
Agency Web Sites
Accounting
Web Crawler To Gather Verification Information
112
Send Notification
108
Enter Application
110
Create Practitioner Record
102
Enter Application
106
View Practitioner Status
104
Complete Application
120
Request, Verification and Audit
122
System Maintenance
124
Verification
FAX Server
114
WebCrawler
Query Accounting
130
100
118

FIG. 2

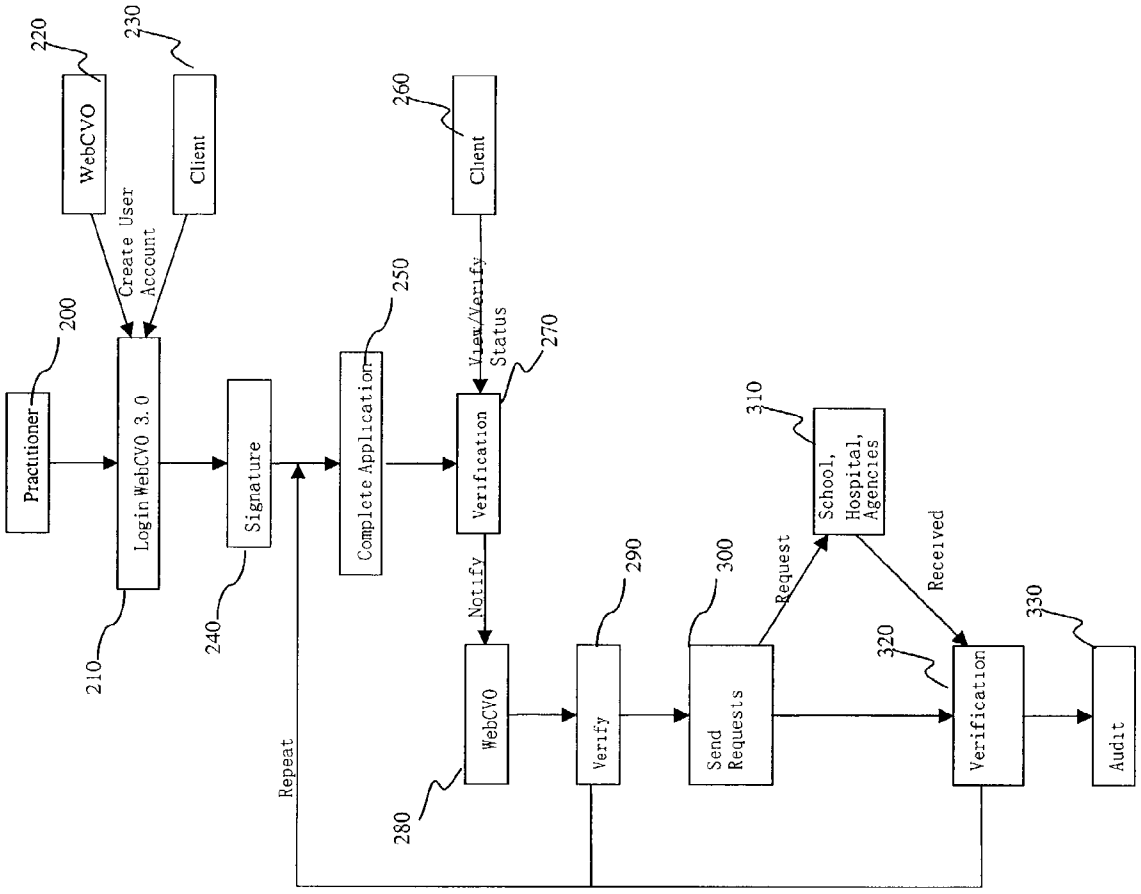

Practitioner
200
Login WebCVO 3.0
210
WebCVO
220
Client
230
Create User Account
Signature
240
Complete Application
250
Client
260
View/Verify Status
270
Verification
Notify
WebCVO
280
Verify
290
Send Requests
300
Request
School, Hospital, Agencies
310
Received
Verification
320
Audit
330
Repeat

FIG. 3

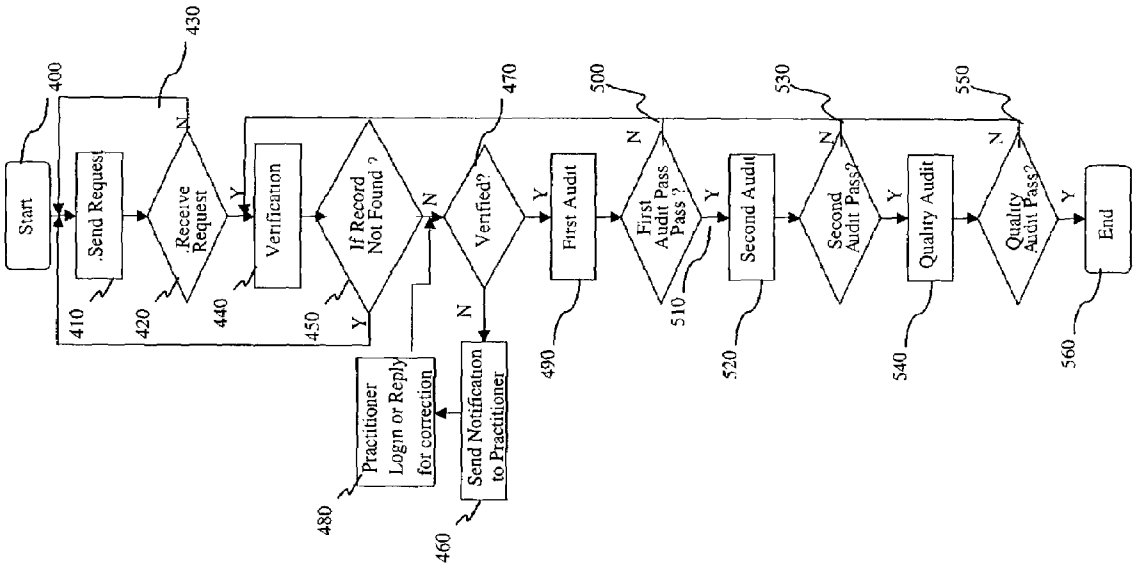

Start
Send Request
Receive Request
Verification
If Record Not Found ?
Verified?
First Audit
First Audit Pass Pass ?
Second Audit
Second Audit Pass?
Quality Audit
Quality Audit Pass?
End
Practitioner Login or Reply for correction
Send Notification to Practitioner
400
410
420
430
440
450
460
470
480
490
500
510
520
530
540
550
560
Y
N

FIG. 4

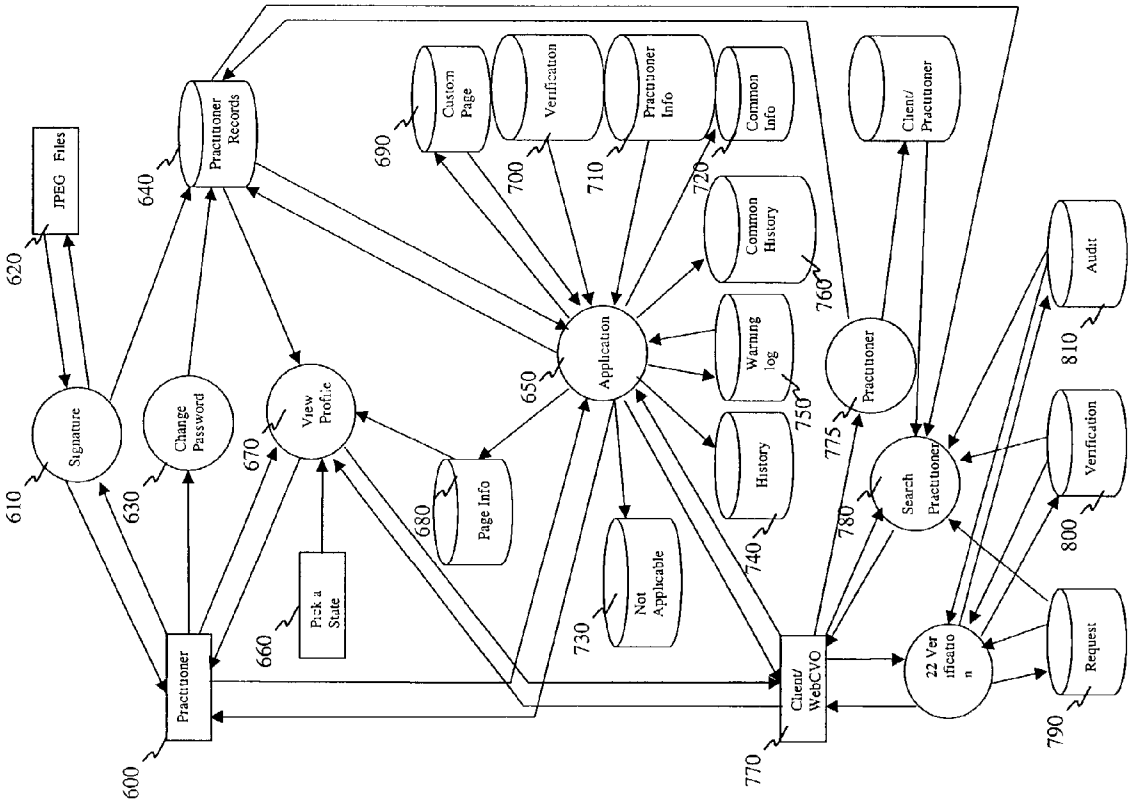

JPEG Files
620
Practitioner Records
640
Custom Page
690
Verification
700
Practitioner Info
710
Common Info
720
Client/ Practitioner
Common History
760
Audit
810
Application
650
Warning log
Practitioner
775
Signature
610
Change Password
630
View Profile
670
Page Info
680
History
750
Search Practitioner
780
Verification
800
Not Applicable
730
740
Pick a State
660
Practitioner
600
Client/ WebCVO
770
22 Verification
Request
790

FIG. 5

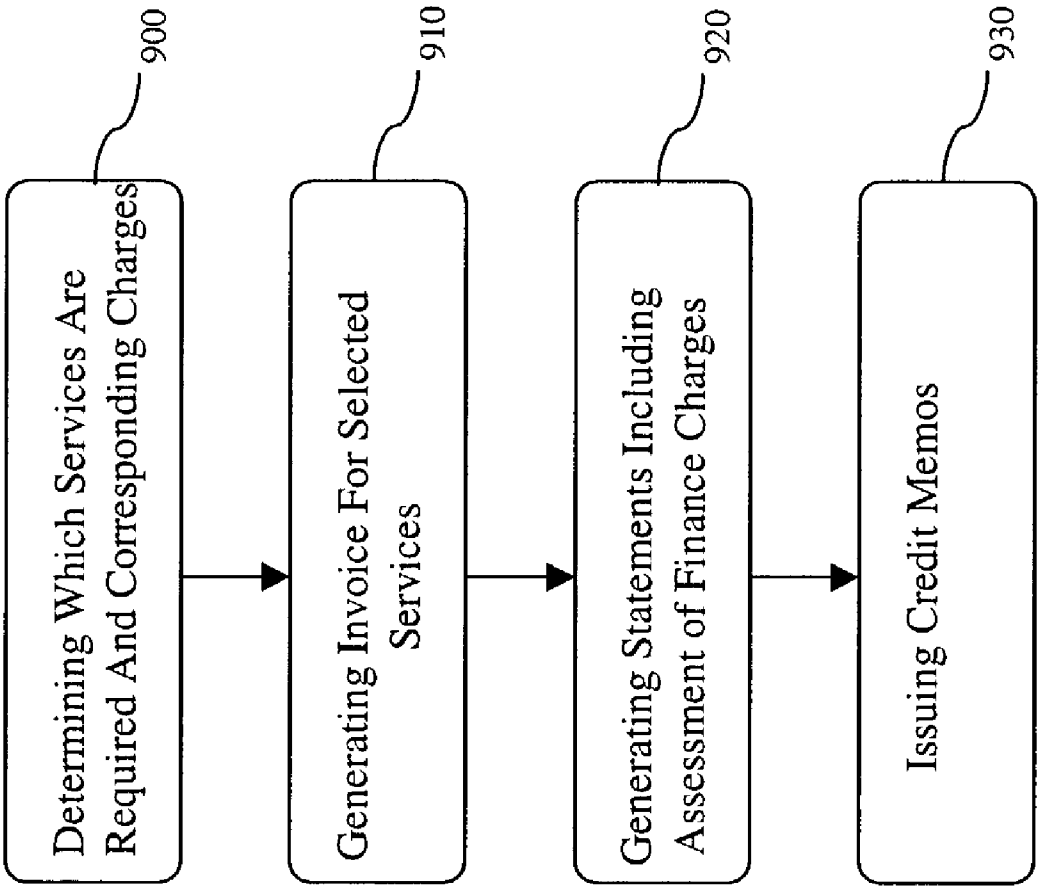

900
Determining Which Services Are Required And Corresponding Charges
910
Generating Invoice For Selected Services
920
Generating Statements Including Assessment of Finance Charges
930
Issuing Credit Memos

FIG. 6

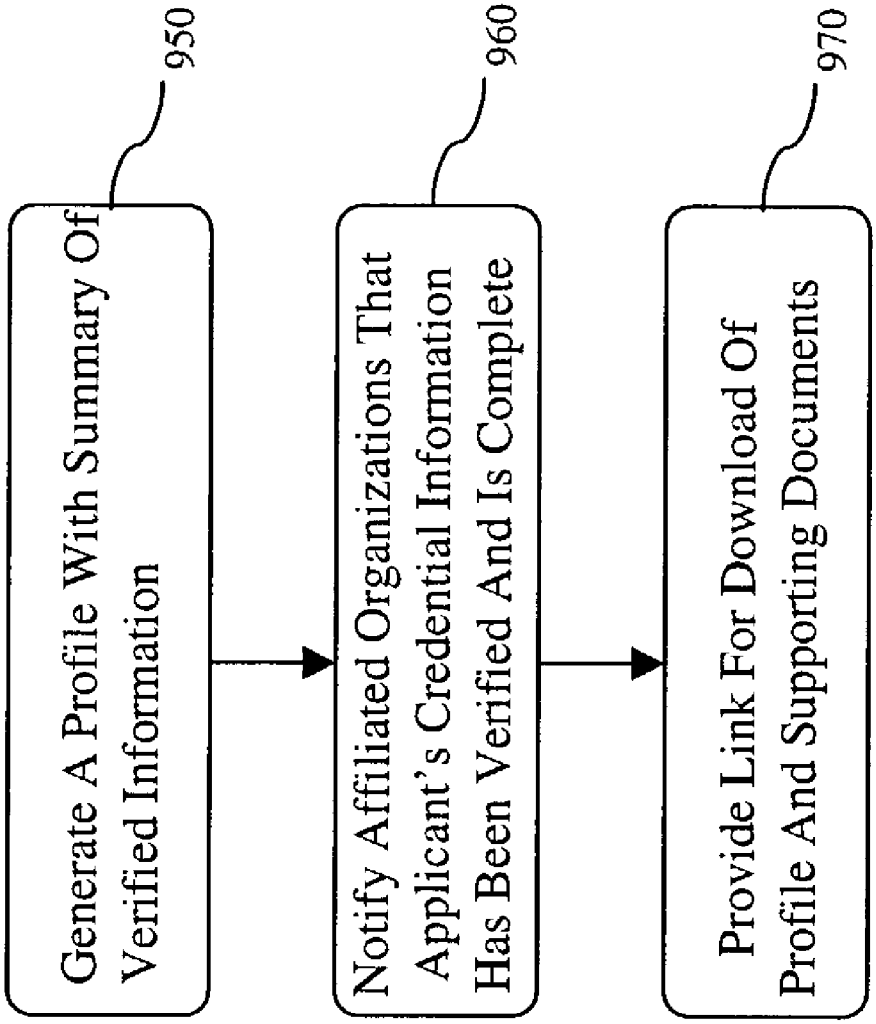

950
Generate A Profile With Summary Of Verified Information
960
Notify Affiliated Organizations That Applicant's Credential Information Has Been Verified And Is Complete
970
Provide Link For Download Of Profile And Supporting Documents

FIG. 7

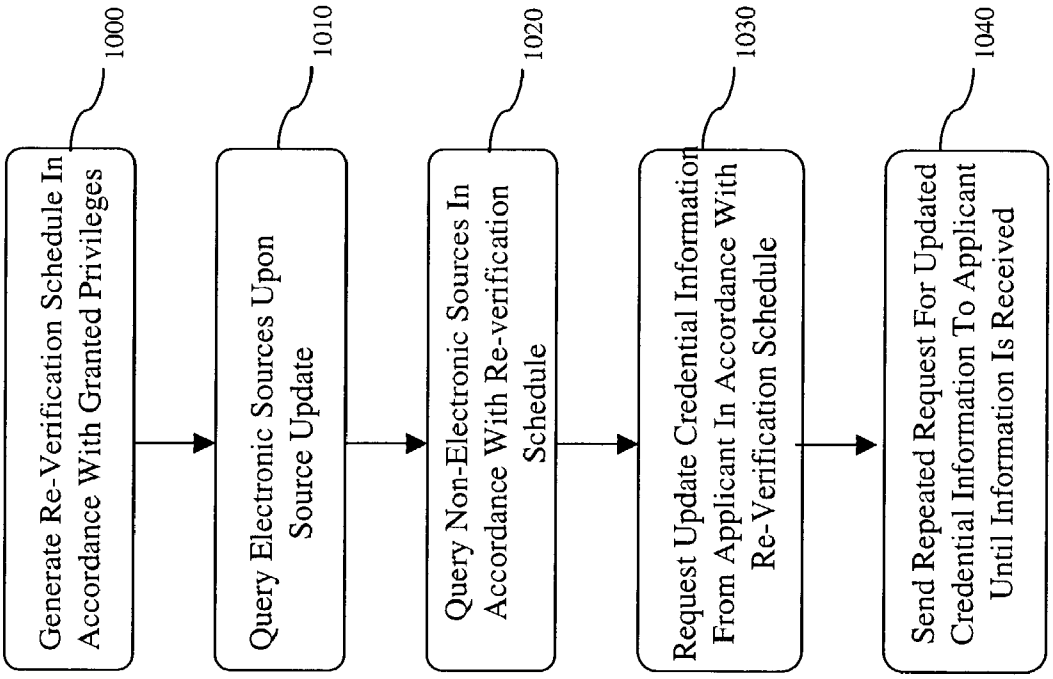

1000
Generate Re-Verification Schedule In Accordance With Granted Privileges
1010
Query Electronic Sources Upon Source Update
1020
Query Non-Electronic Sources In Accordance With Re-verification Schedule
1030
Request Update Credential Information From Applicant In Accordance With Re-Verification Schedule
1040
Send Repeated Request For Updated Credential Information To Applicant Until Information Is Received

FIG. 8

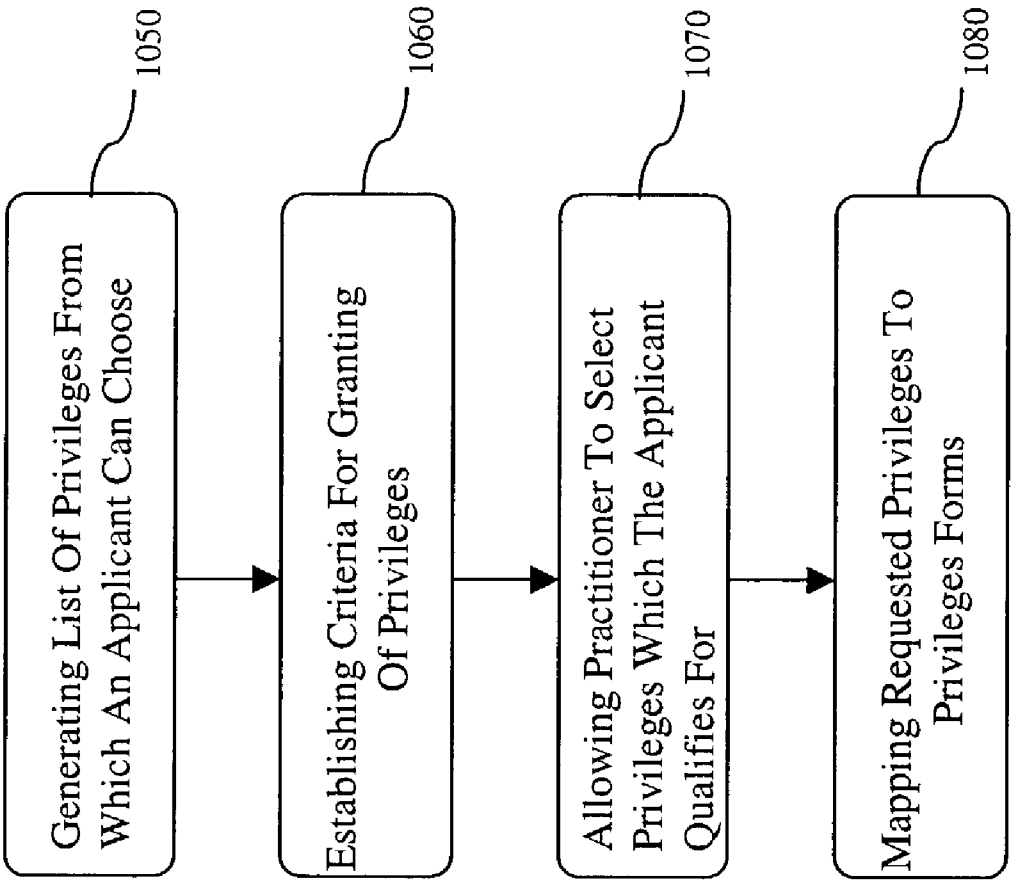

1050
Generating List Of Privileges From Which An Applicant Can Choose
1060
Establishing Criteria For Granting Of Privileges
1070
Allowing Practitioner To Select Privileges Which The Applicant Qualifies For
1080
Mapping Requested Privileges To Privileges Forms

FIG. 9

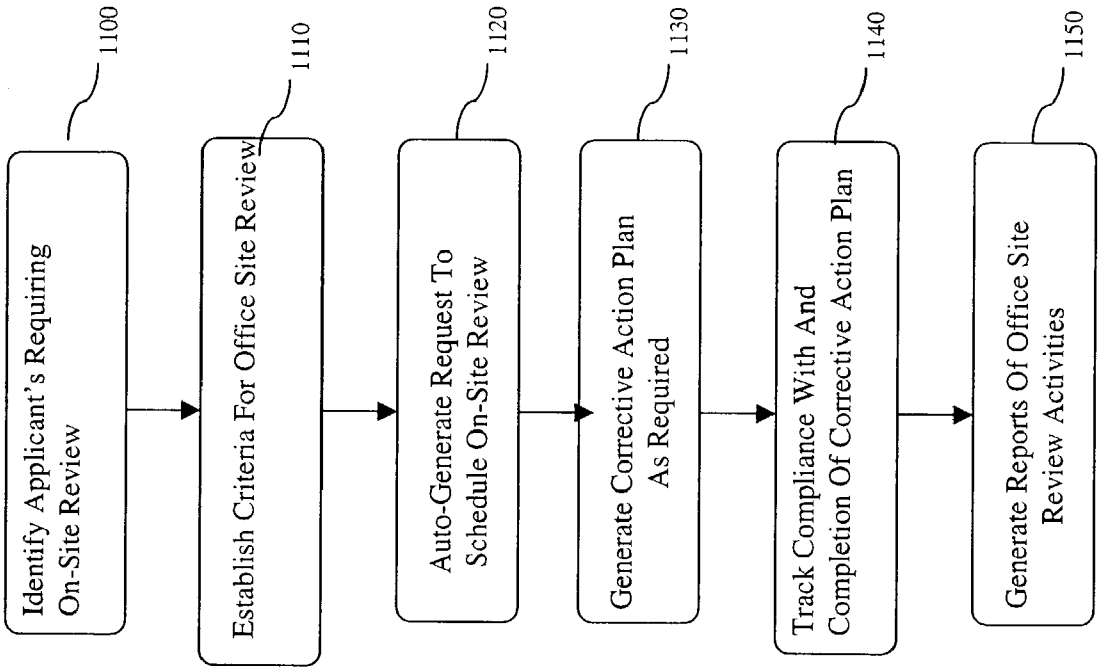

1100
Identify Applicant's Requiring On-Site Review
1110
Establish Criteria For Office Site Review
1120
Auto-Generate Request To Schedule On-Site Review
1130
Generate Corrective Action Plan As Required
1140
Track Compliance With And Completion Of Corrective Action Plan
1150
Generate Reports Of Office Site Review Activities

FIG. 10

ELECTRONIC CREDENTIALS VERIFICATION AND MANAGEMENT SYSTEM

FIELD OF THE INVENTION

The present invention generally relates to electronic management systems, and more particularly, to a system for storing, continually verifying and retrieving credentials records in a global network environment.

BACKGROUND

Professionals are frequently required to be licensed and to undergo rigorous screening before practicing their profession. For example, healthcare practitioners, such as physicians, are typically required by federal, state and regulatory agencies to have a thorough background check when initially applying to hospitals, health maintenance organizations, independent physician associations and other like healthcare entities. In addition, once approved by an entity, the practitioner's background must be re-checked at periodic intervals through the course of his tenure with the healthcare entity. However, practitioner background checks create large volumes of data that must be stored, validated, analyzed and updated on a continuous basis. Such data includes at a minimum, education, training, licensure and license sanctions, work experience, malpractice insurance coverage, malpractice history and peer references.

It may be possible for professional organizations to use electronic data processing systems to automate the creation, use and maintenance of credentials in a manner that is similar to systems currently employed for the storing and management of other occupational data. However, these electronic data processing systems often do not handle data in the wide variety of data formats that may typically be used for credentials verification by healthcare entities. The wide variety of data formats for the collection of credentials information often hinders electronic processing and maintenance of practitioner files. Moreover, many professional practitioners have traditionally used paper-based forms to document their credentials information.

In addition, under current practices there may be significant duplication of credentials information. For example, within healthcare systems similar credentials information may exist in remote practitioner files located at clinics, hospitals, laboratories and physicians' offices. However, due to inefficiencies with current methods of data collection and verification, including the inability of current electronic systems to allow for the sharing of a central record of practitioner data, it is common for practitioner files at one entity to have credentials information that differs from the same practitioner files at another entity within the same system. Such differences may include missing data as well as differing experience, performance and license sanctions histories.

Further, credentials information in the practitioner files is generally not available for review by the practitioners themselves to confirm or dispute the information. Moreover, relationships among specific credentials information documented in a practitioner file such as adverse actions, gaps in work history and misstatements on the credentials application may not be apparent unless manually pulled together as a whole.

In addition, in the current environment, specific credentials information is difficult to access when needed for analysis due to its paper-based nature. Moreover, in current systems the use of a practitioner's file by one entity can preclude its simultaneous use by another entity. Under these circumstances, entities have difficulty ascertaining the fitness of their practitioners to provide services for their customers.

SUMMARY OF THE INVENTION

In one aspect of the present invention a method for electronically verifying information includes requesting credentials information from applicants in a plurality of formats, collecting received credentials information from the applicants in a common format through an interface to a global network, storing collected credentials information in a dynamic database and verifying collected credentials information with external sources through an electronic interface.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will become better understood with regard to the following description, appended claims, and accompanying drawings, in which:

FIG. **1** is a simplified block diagram of an electronic credentials verification system in accordance with an exemplary embodiment of the present invention;

FIG. **2** is a graphical illustration of the relationship of the applicant, client, electronic verification sources and non-electronic verification sources in accordance with an exemplary embodiment of the present invention;

FIG. **3** graphically illustrates the logic flow of an electronic credentialing process in accordance with an exemplary embodiment of the present invention;

FIG. **4** is a flow chart illustrating an audit process for the verification of credentials information in accordance with an exemplary embodiment of the present invention;

FIG. **5** graphically illustrates an online electronic verification process in accordance with an exemplary embodiment of the present invention;

FIG. **6** graphically illustrates a process for creating and maintaining accounting records associated with the verification of credentials information in accordance with an exemplary embodiment of the present invention;

FIG. **7** graphically illustrates a process for generating verified credentials profile information including copies of records from external sources in accordance with an exemplary embodiment of the present invention;

FIG. **8** graphically illustrates a process for creating and maintaining a continuous calendar of re-verification of an applicant's credentials in accordance with an exemplary embodiment of the present invention;

FIG. **9** graphically illustrates a process for allowing applicants to request privileges based upon analysis of credentials information in accordance with an exemplary embodiment of the present invention; and

FIG. **10** graphically illustrates a process for reviewing select practitioner office sites in accordance with an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

An exemplary embodiment of a web based credentials acquisition, storage, verification and audit system (WebCVO) automates and simplifies existing methods of credentials information collection, verification, audit, maintenance and retrieval. In contrast to other systems, the described exemplary embodiment creates and maintains all credentials information electronically and thus can eliminate or supplement the creation and maintenance of physical data records. An exemplary WebCVO may further provide an intuitive, easy-

to-use, web-based interface that allows users to capture and analyze credentials information quickly and efficiently. In accordance with an exemplary embodiment, credentials information may be entered into the electronic credentials system from paper-based forms or may be imported from electronic storage devices (diskette, CD-ROM, tape or the like). Alternatively, credentials information may also be scanned in through the use of a teleform or directly entered by a practitioner into the WebCVO system.

In addition, the described exemplary WebCVO system may include the capability to manage and report on a wide variety of credentials information formats, including credentials information from external sources, such as licensing organizations and governmental databases. In accordance with an exemplary embodiment, the WebCVO system may continuously access external sources to validate current credentials information. The WebCVO system may then alert the practitioner and all entities to which that practitioner is assigned of any information not validated by an external source and to information reported by the source but not recorded in the practitioner's credentials record.

The described exemplary WebCVO system may also prompt practitioners to renew credentials information prior to the expiration of that information. In addition, an exemplary WebCVO system can also incorporate a practitioner's legacy data, such as quality information, into the practitioner record as well as legacy data from mainframe computers.

FIG. **1** illustrates an exemplary electronic credentials system **10**. The described exemplary electronic credentials system **10** includes multiple remote devices **20***a* and **20***b* coupled to one or more web servers **30** through a remote communication network **40**. The communication network may refer to a network or combination of networks spanning any geographical area, such as a local area network, wide area network, regional network, national network, and/or global network. The Internet is an example of a current global computer network. In addition, the communication network may be a hardwire network, wireless network, or a combination of hardwire and wireless networks.

Hardwire networks may include, for example, fiber optic lines, cable lines, ISDN lines, copper lines, etc. Wireless networks may include, for example, cellular systems, personal communications service (PCS) systems, satellite communication systems, packet radio systems, and mobile broadband systems. A cellular system may use, for example, code division multiple access (CDMA), time division multiple access (TDMA), personal digital phone (PDC), Global System Mobile (GSM), or frequency division multiple access (FDMA), among others.

The remote devices **20***a*-**20***b* may be general purpose computing devices that allow users to remotely communicate with the web server over the communication network **40**. The computing devices may be any processor controlled device that permits access to the communication network, including terminal devices, such as personal computers, workstations, servers, clients, mini-computers, main-frame computers, laptop computers, a network of individual computers, mobile computers, palm-top computers, hand-held computers, set top boxes for a television, other types of web enabled televisions, interactive kiosks, personal digital assistants, interactive or web enabled wireless communications devices, mobile web browsers, or a combination thereof.

The computers may comprise one or more input devices such as a keyboard, mouse, touch pad, joystick, pen input pad, and the like. The computers may also possess an output device, such as a visual display and an audio output. One or more of these computing devices may form a computing environment.

An exemplary web server **70** preferably hosts a website **50** comprising one or more interrelated web page files and other files and programs. The files and programs may be accessed via a communications network **40** such as the Internet, by sending for example, a hypertext transfer protocol (HTTP) request specifying a uniform resource locator (URL) that identifies the location of one of said web page files, wherein the files and programs are owned, managed or authorized by a single entity. Such files and programs can include, for example, hypertext markup language (HTML) files, common gateway interface (CGI) files, and Java applications.

In an exemplary embodiment, the web page files preferably include a home page file that corresponds to a home page of the website. The home page can serve as a gateway or access point to the remaining files and programs contained within the website. In one embodiment, all of the files and programs may be located under, and accessible within, the same network domain as the home page file. Alternatively, the files and programs can be located and accessible through several different network domains.

The described exemplary website may use encryption technology such as for example secure socket layer (SSL) encryption and digital certificates to maintain the integrity and confidentiality of electronic transmissions to and from the Web server **70**. In the described exemplary embodiment message data is encrypted using a randomly generated key that is further encrypted using the recipient's public key. This is referred to as the "digital envelope" of the message which is sent to the recipient with the encrypted message. The recipient decrypts the digital envelope using a private key and then uses the symmetric key to unlock the original message.

FIG. **2** graphically illustrates the relationship of the practitioner, client, electronic verification sources and non-electronic verification sources within an exemplary electronic credentials system. The described exemplary electronic credentials system gives users considerable freedom to manage, maintain and utilize the functionality of the system. For example, users **100** can create new practitioner accounts **102** including a credentials application which a practitioner may then complete. In an exemplary embodiment, the system may automatically send a notification **108** to the practitioner preferably instructing the practitioner to log on to the system and input his credentials information **110**.

An exemplary system may send the notification by any of a number of conventional means, such as by email, fax, letter or a combination thereof. In one embodiment an exemplary system may assign a contact method based upon the practitioner's preference for receiving credentials information requests. Further, an exemplary system may automatically send an email to practitioners which includes instructions on how to access the credentials system electronically (e.g. online) as well as requests for the updating or clarifying of credentials information. An exemplary system may compare existing data to newly entered data and archive existing data to a history table.

In one embodiment, the electronic credentials system p may automatically forward a fax with instructions for online access or instructions for receiving a blank credentials application via Internet download, fax or mail to a practitioner. The described exemplary electronic credentials system may also automatically fax or print for mailing complete credentials packages, including instructions and application materials. The described exemplary system may also automatically con-

tact practitioners opting to complete a paper application via fax or letter generation for the completion, update and clarification of their credentials.

In one embodiment a user may also view the status of an existing practitioners **104** credential application or re-verification, plan committee and continuing education meetings and create customized pages for their own use **106**. In addition, the described exemplary system may identify verification requirements for a particular practitioner including the parameters for handling adverse information. The described exemplary system may then automatically contact various entities such as, for example, schools, hospitals, or peers to request verification information **112**, via for example, a web crawler, link, or other conventional method of querying a database.

For example, in an online verification system an encrypted request for verification may be included as parameters on an HTTPS query string to verification sites. In one embodiment the request may further include payment of a verification fee. The described exemplary system may also auto-generate email, fax or letter requests to non-electronic verification sources including payment of verification fees.

An exemplary system may send requests for verification information by fax, letter or email (if choose by phone, an exemplary system may schedule phone calls for WebCVO credentials specialists). An exemplary system may also automatically check the websites of all government agencies (for example, via a web crawler, link or other conventional method of querying a database), or other regulatory bodies for information related to the practitioner's credentials **114**. In addition, an exemplary system may make follow-up requests for verification information according to a pre-set schedule.

The described exemplary system may compare the verification information received from external sources to the credentials information submitted by the applicant. An exemplary system may then auto-update the database with matched information or manually update the database through the use of electronic work prompts or ticklers.

For example, in an exemplary embodiment, a credentials specialist **118** may compile the responses to the requests for verification information and perform various other tasks to complete the application process **120**. A credentials specialist may then utilize a fax server or other similar means to verify and audit the practitioner information **122**.

In an exemplary embodiment, the received verification information may be archived in an online data repository, allowing web access and tracking. For example, in the described exemplary embodiment, electronic information received from verification sites may be stored as digital images in an applicants database. Similarly, verification information received from non-electronic sources may be scanned and stored as scanned images. The described exemplary system may further comprise an accounting component that tracks all individual itemized charges in accordance with particular contract requirements **130**.

An exemplary embodiment of the present invention may also provide instant access to a practitioner's electronic credentials record by authorized entities from any geographic location. For example, the described exemplary system may provide authorized entities to access and update practitioner files using, for example, the Internet. To enable complete replacement of physical records, the present invention permits practitioners to electronically annotate practitioner data. Thus, a practitioner can enter and update credentials information, acknowledge that he or she has reviewed posted credentials information. A practitioner may also provide explanations for any information not validated by an external source or for information reported by a source, not currently posted to the practitioner's record, all by electronically annotating a practitioner's record.

For example, FIG. **3** graphically illustrates the logic flow of an exemplary credentialing process. In one embodiment practitioners **200** may logon to the described exemplary electronically credentialing system **210** and view their own credentials information online. In addition, in an exemplary embodiment the organizations which collect and verify submitted credentials applications may also remotely logon to the system via a global computer network, such as, for example the Internet **220**. In addition, organizations that outsource this responsibility to another organization such as for example, health plans, health systems, hospitals, managed services organizations, preferred provider organizations, medical groups, and independent practice associations may also be provided remote access to the described exemplary system **230**.

The described exemplary system may grant different types of users varying degrees of access to the WebCVO system. In one embodiment the described exemplary system may utilize assigned login IDs and passwords to redirect users to different web pages for different functionalities. In addition, an exemplary system may sign each practitioner record with an electronic signature **240**. This signature may be captured either through electronic creation by the practitioner or by the scanning of a practitioner's actual signature.

An exemplary system may require practitioners to complete all mandatory data fields before submitting a credentials application for verification **250**. An exemplary embodiment of the present invention allows for the assigning of required data fields by practitioner type and verification phase. For example, in one embodiment practitioners may be required to complete a set of data fields pertinent to their field of practice. Practitioners may also be required to complete an initial set of data fields (also pertinent to their field of practice) and upon satisfactory verification of those fields, the practitioner may then be required to complete a secondary, tertiary, etc. set of data fields. In accordance with an exemplary embodiment the required fields are assigned when a practitioner's record is created.

In addition, for applications submitted online, the organization performing credentials verification may view the application and approve it for verification initiation **260**. In practice the described exemplary system may automatically initiate the verification process **270** for submitted applications that are approved for verification **280**.

The described exemplary system may retrieve electronic data from primary source verification websites **290**. The described exemplary system may send requests to non-electronic data sources via email, letter or fax, (or phone) including a copy of a release from the corresponding practitioner with electronic signature and delineation of privileges, if desired **300**.

An exemplary system may correlate the verification information received from external sources with the credentials information entered by the applicant. The described exemplary system may auto-update the database for matched data. In addition, in one embodiment the described exemplary system may attempt to identify reasons for a mismatch between the verification data received from external sources and the credentials information entered by the applicant.

For example, the system may electronically or manually attempt to identify clerical errors, such as typographical errors that may occur during the conversion of a scanned document to text by an optical character recognition program. The system may then request that the applicant provide an explanation for any data mismatches that cannot be attributed

to errors in the data entry or correlation process. An exemplary system may then verify newly entered data by correlating it with the verification information received from the external sources.

In one embodiment, the system may automatically track the receipt of verification information and may automatically re-send verification requests if information is not received. In an exemplary embodiment, time frame intervals for the re-sending of verification requests are determined by the verifying organization. Further, non-responsive sources may be routed to an electronic tickler program for distribution to and follow up by credentials staff.

Non-electronic data sources may return requested verifications through email, fax, letter or the like **310**. The described exemplary system may route information received from non-electronic sources to an electronic work tickler for distribution to and verification by credentials staff **320**. Alternatively, if the verification information is received via teleform it may be auto updated to the database.

In addition, an exemplary system may route mismatched data as well as matched data to an electronic tickler for distribution to and manual verification by credentials staff **290**. In addition, in one embodiment, the described exemplary system may route practitioner information to an audit program to confirm verification was performed correctly **330**. The described exemplary system may utilize a single, double or triple audit process.

For example, FIG. **4** graphically illustrates an exemplary triple audit process. In operation, the described exemplary system may manually or automatically send requests to verifying sources **410** in response to a verification request from a credentialing organization **400**. In one embodiment the system may mark information received in response to verification requests for verification **420**. Otherwise the system may automatically send another request to the verifying sources in accordance with preset time intervals until the requested verification information is received **430**. If a response to the request is not received the system may route the information to an electronic work distribution and reminder program for processing by the credentialing organization.

In practice the credentialing organization or the WebCVO verifies information received from the verifying source **440**. If a verifying source responds with a "Record Not Found" response **450**, the described exemplary system may notify the practitioner via email, fax or letter **460** and ask for corrected information. The practitioner may then respond with corrected information **480** and the system may then send another request to the verifying source **410** with corrected information.

The described exemplary system may route verified credentialing information to an electronic work distribution program for auditor review **490**. In one embodiment, the auditor reviews the verification information received to ensure that it matches that reported on the practitioner's credentials application. If the verification information received matches that reported by the practitioner, the auditor marks the audit as "Pass." In the event the verification information received does not match that reported by the practitioner, the auditor marks the audit as "Fail."

Should the auditor mark the first audit as failed **500**, the original verification is archived and the verification and audit processes are re-initiated. Should the auditor mark the first audit as passed **510**, credentialing information is routed to an electronic work tickler for second auditor review **520**. Should the auditor mark the second audit as failed **530**, the original verification is archived and the verification and audit processes are re-initiated.

In one embodiment, the system may route information that passes two consecutive verification audits to an electronic work distribution program for quality audit review of all verifications **540**. Should the auditor mark the quality audit as failed **550**, the original verification is archived and the verification and audit processes are re-initiated, otherwise the verification audit has been successfully completed **560**.

The described exemplary electronic credentials verification system preferably supports a plurality of data methods of credentials information input. For example, in one embodiment an applicant may enter credentials information from a global computer network such as, for example, the Internet. Alternatively, credentials information may also be imported from a variety of sources such as, for example, a CD-ROM, teleform that is scanned in using optical character recognition, etc. In an exemplary embodiment, the system may require the applicant to provide complete information by continually contacting the applicant via email, fax, letter or a combination thereof until all information is complete.

FIG. **5** graphically illustrates an exemplary online credentials application process. For online application submissions, the described exemplary system may automatically or manually assign a login ID and password to a practitioner **600** for system access. In an exemplary process, a practitioner must review and accept an information release agreement and create a signature **610** after logon to the system. The described exemplary system may capture a scanned signature or an electronic signature for each practitioner and may digitally convert the captured signature to a globally unique identifier (GUID). In one embodiment, a scanned in signature may be saved in JPEG format **620**.

In an exemplary embodiment, the system records the user identification and date and time for each piece of data entered and any and all subsequent changes to provide a complete audit trail for credentials information entered into the system. In this manner, the system transforms a practitioner's credentials application from a static record into a dynamic, real-time comprehensive record that may be linked to enterprise-wide databases to capture or supplement other practitioner data.

In one embodiment, the system may prompt the practitioner to change his or her password **630** and may create a practitioner record by selecting from a set of required data fields that are pertinent to the practitioner's field of practice as well as an initial set of required data fields (also known as a pre-application). When the pre-application is verified an exemplary system may require the practitioner to complete a secondary, tertiary, etc. set of required data fields. An exemplary embodiment of the present invention may also support the creation of practitioner records having additional data fields that are not included in the standard applications stored in the credentials information applications repository **650**.

In the described exemplary embodiment, a practitioner may select credentials applications by state from the application library **660**. In one embodiment, a practitioner may retrieve and view the selected credentials application **670** which is populated with the specific information entered by the practitioner **680**.

The credentials application **650** may comprise a variety of user defined custom pages **690**, the results of the verification processes **700**, as well as additional practitioner data input through modification **710**. An exemplary credentials application may further comprise common data information **720** such as information received from insurance carriers, schools, hospitals, government agencies, etc. The application may also include pages (tabs) that may be marked as not applicable to the particular practitioner **730**, as well as archived data **740**, a warning log comprised of data mis-

matches and identified adverse actions **750** and common field level history tracking data **760**.

In one embodiment the application may be composed of elements that conform to a standardized programming language such as, for example, the extensible markup language (XML) specification. As is known in the art, XML is a markup language for documents containing structured information. Structured information contains both content (words, pictures, etc.) and some indication of what function that content performs. The utilization of a standardized programming language further promotes the automatic utilization of the credentials information across enterprise-wide databases to capture or supplement other practitioner data In one embodiment organizations **770** may have access to practitioner applications **775** and practitioner **775** records **640**. An organization may also search practitioners in the system **780** to retrieve and review requested information **790**, verification information **800** and audit information **810**. Organizations may also access practitioner verification information to view the status and detailed information **820**.

Referring to FIG. **6**, an exemplary embodiment of the present invention may create and maintain accounting records associated with the verification of credentials information. For example, the described exemplary system may determine which services are required for a particular client as well as the charges associated with those services **900**. The described exemplary embodiment may then automatically generate an invoice for the appropriate services when they are performed. **910**. The system may also generate accounting statements in accordance with the appropriate services including assessments of finance charges where appropriate **920**. The system may then automatically issue credit memos **930** from the accounting statements **930**.

Referring to FIG. **7**, an exemplary embodiment of the present invention may also generate verified credentials profile information including copies of all records from external sources. For example, in one embodiment, the described exemplary system may generate a profile with a synopsis of verified information as required by regulatory agencies within the field of practice of the applicant **950**. The describe exemplary system may also notify affiliated organizations that the applicant's credentials information has been verified or re-verified and is complete. The system may also provide a hyperlink **970** to a site from which interested parties may download the verified credentials profile. The system may further make copies of the electronic and scanned documents utilized in the verification process available for download as well.

Referring to FIG. **8** an exemplary embodiment of the present invention may also create and maintain a continuous calendar of re-verification of an applicant's credentials information. For example, an exemplary system may create a re-verification schedule in accordance with the requirements for re-verification for a particular set of privileges **1000**. The described exemplary system may then query electronic sources **1010** and non-electronic sources in accordance with the prescribed schedule **1020**. The described exemplary system may also request that the applicant update credentials information on a prescribed schedule **1030** and continually send repeated requests for updated information until the requested information is received **1040**.

Referring to FIG. **9** an exemplary embodiment of the present invention may also allow applicants to request privileges based upon analysis of credentials information. For example an exemplary system may generate a list of privileges from which a practitioner in a particular field may select **1050**. The described exemplary system may then establish criteria such as, for example, level of education, training and experience for the granting of each privilege **1060**. The system may then compare the applicant's credentials with the required criteria and restrict the privileges which the applicant may select from to those for which the applicant has satisfied the specified criteria **1070**. The system may then map the requested privileges to appropriate privileges forms **1080** which may then be automatically sent via email, fax or letter to external sources for review of competence.

In an online system, a "pop up" message may be generated when an applicant attempts to select a privilege which the applicant does not qualify for. The pop message may provide the reasons for privilege ineligibility. Alternatively, an exemplary system may auto-generate an email, fax or letter to the applicant that provides the reasons for privilege(s) ineligibility.

Referring to FIG. **10**, an exemplary embodiment of the present invention may also allow for the review of select practitioner office sites. For example, in one embodiment an exemplary system may identify practitioners requiring office site review to satisfy the regulatory requirements, etc **1100**. The system may then establish the criteria for the on-site review in accordance with the requirements for regulatory compliance **1100**. The system may then auto-generate a request to schedule an on-site review **1120**, generate review results and generate a corrective action plan, if required as a result of the review **1130**. An exemplary system may track compliance with and completion of the corrective action plans **1140** and generate a report of the office site review activities **1150**.

The invention described herein will itself suggest to those skilled in the various arts, alternative embodiments and solutions to other tasks and adaptations for other applications. It is the applicants' intention to cover by claims all such uses of the invention and those changes and modifications that could be made to the embodiments of the invention herein chosen for the purpose of disclosure without departing from the spirit and scope of the invention.

What is claimed is:

1. A method for electronically verifying information pertaining to applicants over a communication network including a plurality of computing devices, the method comprising:

collecting credentials information pertaining to applicants in one or more of a plurality of formats;

converting credentials information in one or more of the plurality of formats into a common format of collected credentials information;

storing the collected credentials information in a dynamic relational database; and

verifying concurrently for a plurality of applicants the collected credentials information with external sources through an electronic interface, wherein the verifying further comprises:

automatically obtaining third party credentials data wherein the obtaining comprises querying automatically on a periodic basis third party databases having third party credentials data relating to the collected credentials information; and

automatically electronically comparing the obtained third party credentials data to the collected credentials information pertaining to the applicant;

automatically electronically updating the relational database with the retrieved data;

automatically electronically notifying a user of inconsistencies between the obtained third party credentials data and the collected credentials information pertaining to the applicant; and

providing selective electronic access to the updated third party credentials information over the communication network to one or more users and to the applicant to which the third party credentialing information pertains.

2. The method of claim **1** further comprising creating and maintaining a re-verification calendar of said credentials information.

3. The method of claim **1** further comprising identifying adverse information or errors in verification of credentials information.

4. The method of claim **1** further comprising auditing credentials information.

5. The method of claim **1** further comprising generating user-defined reports on credentials information.

6. The method of claim **1** further comprising generating accounting records associated with the verification of credentials information.

7. The method of claim **1** wherein collecting credentials information in a plurality of formats comprises:

creating an applicant record for data storage;

contacting the applicant via email, fax, letter or a combination thereof; and

providing the applicant with reminder renewals for expiring credentials information.

8. The method of claim **1** wherein collecting credentials information comprises collecting responses over the Internet.

9. The method of claim **1** wherein collecting credentials information comprises collecting response information stored on a storage media.

10. The method of claim **1** wherein collecting credentials information comprises importing teleform data.

11. The method of claim **1** wherein collecting credentials information comprises continually requesting credentials information from the applicant via email, fax, letter or a combination thereof until all of the requested credentials information is collected.

12. The method of claim **1** further comprising authenticating the credentials information with an electronic or scanned signature.

13. The method of claim **12** wherein authenticating the credentials information with an electronic signature or scanned signature comprises:

assigning a Global Unique Identification (GUID) upon login; and

capturing the scanned signature from a paper document.

14. The method of claim **1** wherein storing collected credentials information in a dynamic database comprises:

time-stamping collected credentials information;

comparing existing credentials information to newly entered credentials information; and

archiving existing credentials information to a history table.

15. The method of claim **1** further comprising creating client specific dynamic template in accordance with extensible markup language specification and mapping stored credentials information into dynamic template.

16. The method of claim **1** wherein verifying collected credentials information with external sources further comprises:

auto-generating verification requests to non-electronic sources; and

receiving verification information from non-electronic sources and storing as scanned images.

17. The method of claim **16** wherein verifying collected credentials information with external sources further comprises:

comparing verification information with credentials information submitted by the practitioner;

auto-updating the database with matched information;

manually updating the database through the use of electronic work ticklers; and

providing real-time notification of adverse information.

18. The method of claim **3** wherein identifying adverse information or errors in verification of credentials information comprises:

requesting explanations for adverse information or errors from the practitioner; and

re-verifying the credentials information, if warranted.

19. The method of claim **4** wherein auditing credentials information comprises:

(a) performing two consecutive audits of verified credentials information;

(b) performing a quality audit of selected credentials information if each of the two consecutive audits is passed; and

(c) repeating steps (a) and (b) if either of the two consecutive audits is not passed or if the quality audit is not passed.

20. The method of claim **1** further comprising:

generating a list of a plurality of privileges;

establishing criteria for granting said plurality of privileges;

allowing practitioner to select privileges for which he is qualified;

generating delineation of privileges forms from selected privileges;

and auto-sending such delineation of privileges forms to external sources for verification of competence.

21. The method of claim **1** further comprising:

identifying applicants requiring office site review;

performing data entry of office site review results;

generating corrective action plans if required;

tracking completion of corrective action plans; and

generating reports of office site review activities.

22. The method of claim **1** further comprising:

generating a profile of verified credentials information required by regulatory agencies;

notifying affiliated organizations that the credentials information has been verified or re-verified and is complete; and

providing a hyperlink for download of the profile and all copies of electronic and scanned documents utilized in the verification process.

23. An electronic credentials verification system, comprising:

means for requesting credentials information pertaining to applicants in one or more of a plurality of formats;

means for collecting credentials information pertaining to the applicants through an interface to a communication network;

means for storing collected credentials information in a dynamic database; and

means for automatically verifying collected credentials information with external sources through an electronic interface, wherein the means for verifying comprises:

means for automatically obtaining third party credentials data, wherein the means for automatically obtaining comprises means for querying automatically on a periodic basis third party databases having third party credentials data relating to the collected credentials information; and

means for automatically electronically comparing the obtained third party credentials data to the collected credentials information pertaining to the applicant;

means for automatically electronically updating the dynamic database with the retrieved data and images

means for automatically electronically notifying a user of inconsistencies between the obtained third party credentials data and the collected credentials information pertaining to the applicant; and

means for automatically presenting the user with the updated third party credentialing information.

24. The electronic verification system of claim **23** further comprising means for allowing for selection of privileges based upon analysis of credentials information.

25. The electronic verification system of claim **23** further comprising means for reviewing office sites of select applicants.

26. The electronic verification system of claim **23** further comprising means for generating verified credentials profile information including copies of records from external sources.

27. The electronic verification system of claim **23** further comprising means for creating and maintaining a calendar of re-verification of an applicant's credentials.

28. The electronic verification system of claim **23** further comprising means for generating client specific dynamic credentials application templates with the stored credentials information.

29. The method of claim **1** further comprising providing the applicants a means to comment on the inconsistencies between the obtained third party credentials data and the collected credentials information pertaining to the applicant.

30. The electronic verification system of claim **23** further comprising means for commenting on the inconsistencies between the obtained third party credentials data and the collected credentials information pertaining to the applicant.

31. The method of claim **1** wherein the providing selective electronic access comprises making one or more images of primary source data pertinent to the presented information available through download or hyperlink.

32. The method of claim **1** wherein the means for presenting comprises means for making one or more images of primary source data pertinent to the presented information available through download for hyperlink.

33. The electronic verification system of claim **23** wherein the means for presenting comprises means for making one or more images of primary source data pertinent to the presented information.

34. The method of claim **1** wherein the means for presenting comprises means for presenting one or more images of primary source data pertinent to the presented information.

35. The method of claim **1** wherein the querying automatically on a periodic basis third party databases having third party credentials data relating to the collected credentials information comprises continuously querying the third party databases.

36. The electronic verification system of claim **23** wherein the means for querying automatically on a periodic basis third party databases having third party credentials data relating to the collected credentials information comprises means for continuously querying the third party databases.

* * * * *

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY

This case has been assigned to District Judge Margaret M. Morrow and the assigned discovery Magistrate Judge is Rosalyn M. Chapman.

The case number on all documents filed with the Court should read as follows:

CV09- 5031 MMM (RCx)

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

All discovery related motions should be noticed on the calendar of the Magistrate Judge

---

NOTICE TO COUNSEL

A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).

Subsequent documents must be filed at the following location:

[X] Western Division
312 N. Spring St., Rm. G-8
Los Angeles, CA 90012

[ ] Southern Division
411 West Fourth St., Rm. 1-053
Santa Ana, CA 92701-4516

[ ] Eastern Division
3470 Twelfth St., Rm. 134
Riverside, CA 92501

Failure to file at the proper location will result in your documents being returned to you.

Name & Address: Gary Dukarich, SBN 188561
Christie, Parker & Hale, LLP
3501 Jamboree Road
Suite 6000
Newport Beach, Ca 92660
(949) 476-0757

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

Medversant Technologies, L.L.C.

PLAINTIFF(S)

v.

Morrisey Associates, Inc.

DEFENDANT(S).

CASE NUMBER

CV09-05031 MMM (RCx)

SUMMONS

TO: DEFENDANT(S): _____

A lawsuit has been filed against you.

Within 20 days after service of this summons on you (not counting the day you received it), you must serve on the plaintiff an answer to the attached ☑ complaint ☐ _____ amended complaint ☐ counterclaim ☐ cross-claim or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff's attorney, Gary Dukarich, whose address is 3501 Jamboree Road, Suite 6000, Newport Beach, Ca 92660 (949) 476-0757. If you fail to do so, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Clerk, U.S. District Court

Dated: JUL 13 2009

By: LA'REE HORN
Deputy Clerk

(Seal of the Court)

1192

[Use 60 days if the defendant is the United States or a United States agency, or is an officer or employee of the United States. Allowed 60 days by Rule 12(a)(3)].

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA

CIVIL COVER SHEET

I (a) PLAINTIFFS (Check box if you are representing yourself ☐)

Medversant Technologies, L.L.C.

DEFENDANTS

Morrisey Associates, Inc.

(b) Attorneys (Firm Name, Address and Telephone Number. If you are representing yourself, provide same.)

Gary Dukarich, SBN 188561
Christie, Parker & Hale, LLP, 3501 Jamboree Road, Suite 6000
Newport Beach, CA 92660, Tel.: (949) 476-0757

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an X in one box only.)

☐ 1 U.S. Government Plaintiff ☑ 3 Federal Question (U.S. Government Not a Party)

☐ 2 U.S. Government Defendant ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES - For Diversity Cases Only (Place an X in one box for plaintiff and one for defendant.)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated or Principal Place of Business in this State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated and Principal Place of Business in Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. ORIGIN (Place an X in one box only.)

☑ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify): ☐ 6 Multi-District Litigation ☐ 7 Appeal to District Judge from Magistrate Judge

V. REQUESTED IN COMPLAINT: JURY DEMAND: ☑ Yes ☐ No (Check 'Yes' only if demanded in complaint.)

CLASS ACTION under F.R.C.P. 23: ☐ Yes ☑ No ☑ **MONEY DEMANDED IN COMPLAINT: $** TBD

VI. CAUSE OF ACTION (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)

15 U.S.C. §271 - Patent Infringement

VII. NATURE OF SUIT (Place an X in one box only.)

OTHER STATUTES
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce/ICC Rates/etc.
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 810 Selective Service
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 875 Customer Challenge 12 USC 3410
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Act
- ☐ 892 Economic Stabilization Act
- ☐ 893 Environmental Matters
- ☐ 894 Energy Allocation Act
- ☐ 895 Freedom of Info. Act
- ☐ 900 Appeal of Fee Determination Under Equal Access to Justice
- ☐ 950 Constitutionality of State Statutes

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loan (Excl. Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS
PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Fed. Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury-Med Malpractice
- ☐ 365 Personal Injury-Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus-Alien Detainee
- ☐ 465 Other Immigration Actions

TORTS
PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

CIVIL RIGHTS
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/Accommodations
- ☐ 444 Welfare
- ☐ 445 American with Disabilities - Employment
- ☐ 446 American with Disabilities - Other
- ☐ 440 Other Civil Rights

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence Habeas Corpus
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus/ Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition

FORFEITURE / PENALTY
- ☐ 610 Agriculture
- ☐ 620 Other Food & Drug
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 630 Liquor Laws
- ☐ 640 R.R. & Truck
- ☐ 650 Airline Regs
- ☐ 660 Occupational Safety /Health
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 730 Labor/Mgmt. Reporting & Disclosure Act
- ☐ 740 Railway Labor Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☑ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS-Third Party 26 USC 7609

FOR OFFICE USE ONLY: Case Number: CV09-05031

AFTER COMPLETING THE FRONT SIDE OF FORM CV-71, COMPLETE THE INFORMATION REQUESTED BELOW.

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

VIII(a). IDENTICAL CASES: Has this action been previously filed in this court and dismissed, remanded or closed? ☑ No ☐ Yes
If yes, list case number(s): _____

VIII(b). RELATED CASES: Have any cases been previously filed in this court that are related to the present case? ☑ No ☐ Yes
If yes, list case number(s): _____

Civil cases are deemed related if a previously filed case and the present case:
(Check all boxes that apply) ☐ A. Arise from the same or closely related transactions, happenings, or events; or
☐ B. Call for determination of the same or substantially related or similar questions of law and fact; or
☐ C. For other reasons would entail substantial duplication of labor if heard by different judges; or
☐ D. Involve the same patent, trademark or copyright, and one of the factors identified above in a, b or c also is present.

IX. VENUE: (When completing the following information, use an additional sheet if necessary.)

(a) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named plaintiff resides.
☐ Check here if the government, its agencies or employees is a named plaintiff. If this box is checked, go to item (b).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles	

(b) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named defendant resides.
☐ Check here if the government, its agencies or employees is a named defendant. If this box is checked, go to item (c).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
	Illinois

(c) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** claim arose.
Note: In land condemnation cases, use the location of the tract of land involved.

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles	

*** Los Angeles, Orange, San Bernardino, Riverside, Ventura, Santa Barbara, or San Luis Obispo Counties**
Note: In land condemnation cases, use the location of the tract of land involved

X. SIGNATURE OF ATTORNEY (OR PRO PER): _____ Date 7/13/09

Notice to Counsel/Parties: The CV-71 (JS-44) Civil Cover Sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law. This form, approved by the Judicial Conference of the United States in September 1974, is required pursuant to Local Rule 3-1 is not filed but is used by the Clerk of the Court for the purpose of statistics, venue and initiating the civil docket sheet. (For more detailed instructions, see separate instructions sheet.)

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405(g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405(g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. (g))