METHOD AND SYSTEM TO COLLECT NETWORK ADDRESSES AND TRANSFER THEM TO A NETWORK SYSTEM

Inventor: Carlos de la Huerga, Milwaukee, WI (US)

Filed: May 9, 2011

Related U.S. Application Data
Continuation of application No. 10/899,520, filed on Jul. 26, 2004, now Pat. No. 7,941,534, which is a continuation of application No. 09/170,169, filed on Oct. 13, 1998, now Pat. No. 6,408,330.

Publication Classification
Int. Cl.
G06F 15/173 (2006.01)

U.S. Cl. ........................................... 709/223

ABSTRACT
An information system network and method for use thereof for remotely gathering network addresses and sending a message to a network address, the system including at least a remote information collecting device and a network including an input device and a network device, the collecting device in remotely gathering network address and transferring the network address to the input device to be sent to a corresponding network device.
Figure 8

Base Contents:

Minimum Information:
Password or Private/Public Security Key(s)

Optional Information:
User Name
User ID number
User database address
Battery Replacement Date
Device Disabled
List of Additional Memory Contents
Hospital specific information
HTML formats or Java applets
Access Privileges
Occupation and specialty
Public key and other identification information for each
Security Verification System the security badge can
be used with

Figure 9

Patient Identification Information:

Minimum Information:
Patient ID number

Optional Information:
Patient's name
Patient's database address
Medical Record Number
Sex
Age
Weight
Height
Figure 10

Medication Information:

Minimum Information:
- Medication name(s)
- Quantity of medication dispensed in the container

Optional Information:
- Patient's ID and/or name
- Patient's database address
- Date and time read
- Date and time dispensed
- Date and time given
- Pharmacy prescription number
- Pharmacy medication dispensing number
- Person dispensing medication
- Data base address of person dispensing medication
- Physician Authorized to Dispense Medication

Figure 11

Dictation Information:

Minimum Information:
- User Identification
- Date and time of dictation
- Length of dictation
- Digitized dictation

Optional Information:
- Patient's ID and/or name
- Patient's database address
### Monitoring or Treatment Device Information:

<table>
<thead>
<tr>
<th>Minimum Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and time information gathered</td>
</tr>
<tr>
<td>Device identification and location</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Optional Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient's ID and/or name</td>
</tr>
<tr>
<td>Patient's database address</td>
</tr>
<tr>
<td>Device settings</td>
</tr>
<tr>
<td>Device measurements or readings</td>
</tr>
</tbody>
</table>

**Figure 12**

```
```

**Figure 13A**
<html>
<body>

ID: 987654321
Date: 13:59 19-May-1996
Report Type: Medication Administration

Medication Given:

<table>
<thead>
<tr>
<th>Medicine</th>
<th>Dosage</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penicillin</td>
<td>100mg</td>
<td>2 capsules</td>
</tr>
<tr>
<td>Tylenol w/Codeine</td>
<td>200mg</td>
<td>1 capsule</td>
</tr>
</tbody>
</table>

ID Device Serial Number: 1265338

</body>
</html>
<html>
<head>
<title>Medication Administration</title>
</head>

Report type: Medication Administration<br>
Patient ID Verified: YES<br>

<table>
<thead>
<tr>
<th>Medication Given</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penicillin</td>
<td>2, 1.5, 1, 0.5</td>
</tr>
<tr>
<td>TYLENOL W/ Codeine</td>
<td>1, 0.5, none</td>
</tr>
</tbody>
</table>

Given by:<br>

Dispensed by:<br>

ID Device Serial Number: 1265338

Figure 14A
Attesip to decryst resperse assi se serification algorithra to cesterg&re sessits wity the systesses&ter sigra.

Figure 15A
Check First Attempt

Is the computer system set to require a keyboard entered password?

Prompt system user to enter password.

Was correct password entered?

Have there been 3 consecutive failed password attempts?

Figure 15B
Enable the recognition of this user's security badge by the computer system. Notify system security administration of a possible attempt to breach security, identifying the security badge and the computer terminal where the attempt occurred.

Go to Request Response

Log the user onto the computer system. Provide the user access to databases and program features as allowed.

Transfer data records, if any, stored and flagged by security badge for transfer to a database

Wait temporarily before transmitting next signal

Transmit recommitment signal.
Is value great enough to logout the system user?

Log user off. Overwrite and delete any memory cache or temporary workspace used by user or application program run by the user.

Decrypt and process response through verification algorithm and compare to original recommitment signal.

Does output of verification algorithm match original recommitment signal?

Figure 15E
The original system user is still using the computer system. Reset the idle / invalid link counter and restore screen and processor to normal operation if it was previously disabled.

Go to Wait

The output of the verification algorithm matches the identity of another user.

Is the counter value greater than a third limit?

Yes

Go to Wait

A new user is recognized, but the current user has not been away long enough yet

No

Log original system user off the computer system. Overwrite and delete any memory cache or temporary workspace used by user or application program run by the user. Logon new system user.

Go to Check
First Attempt

Figure 15F
Figure 16A

Wait for Message

Wait to receive a signal

Has a signal been received during the wait state?

YES

NO

Turn power off for a period of time, and return to power on state

Process and identify signal

Is signal a general request for response?

YES

NO

Is signal addressed to this electronic security badge?

YES

NO

J

K
Figure 16B
Use the signal's key identification to locate the public key and decrypt the signal.

Can the decrypted signal be confidently identified as originating from the Verification System?

- **YES**: Return invalid message code
- **NO**: Go to Wait for Message

Process signal through encryption algorithm

Transmit re-encrypted signal back to computer terminal.

Go to Wait for Message

Figure 16C
Is signal prompting security badge to transmit stored data records to the computer system?

- **NO**
  - Go to Wait for Message

- **YES**
  - Send requested data
  - Go to Wait for Message

Is signal a prompt to delete data?

- **No**
  - Go to Wait for Message

- **Yes**
  - Delete data specified
  - Go to Wait for Message

Figure 16D
Is signal prompting system user to digitally sign a data record

Prompt user to press the activation button on the electronic security badge

Wait temporarily for button to be pressed

Has the button been pressed?

Send message indicating signature not provided

Go to Wait for Message

Figure 16E
Encrypt entire document or a special control portion of the document and transmit back to the computer terminal

Go to Wait for Message

Figure 16F
Figure 17A

User presses activation button.

Is the electronic security badge associated with a patient?

Electronically security badge transmits identification information and a request for data to be returned.

Electronic security badge transmits identification information and patient identification information and a request for data to be returned.

Wait temporarily for a response signal from security badge.

Any response signal?

Terminate data request process.
Figure 17B
Figure 17C

1. **Associate the electronic security badge with the newly received patient. Add date and time to patient information. Start timer to cancel patient association.**

2. **Data acquisition completed**

3. **Has the electronic security badge been associated with a patient?**
   - **Yes**
     - **Modify data record, generate database address, and emit sound to indicate successful transaction.**
     - **Data acquisition completed**
   - **No**

4. **Modify data record, generate database address if patient ID information is available and emit sound to indicate a successful transaction.**

**Data acquisition completed**
User presses the dictation button

User dictates desired message. It is digitized and stored for later transfer

Has the electronic security badge been associated with a patient?

Add date and time to record and patient identification information previously recorded. Indicate data type is dictation, combine user identification number, patient identification and date and time to formulate a database address to store this data. Emit sound indicating successful transaction.

Dictation completed

Add date and time to record. Indicate data type is dictation, combine user identification number, date and time to formulate a generic dictation database address to store this data. Emit sound indicating successful transaction.

Dictation completed

Figure 18
Figure 20
Start

NO
Signature Required?

YES
Transmit Document to ICD for Signature

NO
Document Returned?

YES
Document Signed?

NO
Indicate Unsigned

YES
Store Document

Figure 25
Start

Document Received?

YES

DC < TDC?

NO

Add Random Text to Document Generating New DC

NO

Apply Digital Signature to Document Generating New DC

YES

Retrieve Standard Mark and Modify as \( f(\text{DC}) \)

Apply Modified Mark to Digital Signature Generating Water Marked Signature

Replace Digital Signature with Water Marked Signature in Document

Transmit “Signed” Document to Terminal

END

Figure 26
Start

1. Display Document with Signature and Authentication Icon
2. NO Authenticate Selected?
   - Yes
     - Identify Water Marked Digital Signature
     - Transmit Authenticate Request and Water Marked Signature
   - No
     - Re-generate Document Received?
     - Yes
       - Display Suspect and Re-generated Documents
     - No
       - Authenticate Selected?
         - Yes
           - Indicate Authenticate
         - No
           - Indicate No Authenticate

END

Figure 27
Start

Receive Authenticate Request and Signature

Retrieve Standard Mark and Signature from Memory

Remove Standard Mark and Signature

Expand Content Mark Into Re-generated Document

Transmit Re-generated Document

END

Figure 28
METHOD AND SYSTEM TO COLLECT NETWORK ADDRESSES AND TRANSFER THEM TO A NETWORK SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of application Ser. No. 10/899,520 “System and method to authenticate users to computer systems” which was filed on Jul. 26, 2004, which was a continuation of application Ser. No. 09/170,169 related to the earlier filed patent application entitled “Data Collection Device and System” which was filed on Oct. 13, 1998 now U.S. Pat. No. 6,408,330.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not applicable.

BACKGROUND OF THE INVENTION

The present invention relates to computer systems for the management of information distributed across a plurality of electronic system devices. More particularly, the invention relates to a system which includes a plurality of network servers, interface terminals, remote data collecting devices and other smart devices to facilitate information collection, approval, editing and storage such that the network server storage location of specific information can be specified using a remote collecting device. The invention also relates to record verification methods.

As an initial matter, in the interest of simplifying this explanation and unless indicated otherwise, the description which follows describes the invention in the context of a medical facility. However, it should be recognized that the invention should not be so limited and clearly has applications which are outside a medical facility, only some of which are specifically discussed hereinafter.

In many industries a need exists for remote information collection and information storage which facilitates easy subsequent information retrieval. For example, in medical facilities there is a need, for purposes of patient protection, quality control, record keeping, billing, and forensics, to monitor, control, and record access to medicine dispensation, medicine administration, IVs, blood transfusions, and other treatments as well as the collection, administration, and testing of blood and tissue samples. These events have traditionally been controlled and monitored manually by doctors, nurses and other facility personnel (hereinafter “physicians” generally).

Unfortunately the increasing specialization and complexity of medical care has vastly increased both the types and amount of routine record keeping that is required to track all events which occur in a facility. Advantageously, rapid growth of computer technologies has provided tools which can be used to store and retrieve specific information from a vast quantity of medical records. In particular, Internet technology is now routinely used to create hospital Intranets, link discrete hospital databases and make their data, images, and audio video records commonly accessible.

Most medical facility Intranet systems include a plurality of network servers disposed in either one central information systems department or at various locations throughout the facility, a plurality of computer terminals located throughout the facility and a data bus which links all of the servers and computers together. Software is loaded onto each computer to facilitate information entry and specify server addresses for information retrieval and storage.

The first Intranet systems were used for only very few applications and therefore were not extremely complex. However, over time, as Intranet applications became more numerous and their use as information management tools became more widely recognized, single server systems could no longer meet the information management needs of even a single medical facility. This information management capacity problem has been exacerbated by prolific mergers and acquisitions among medical groups such that many medical groups now have several locations and vast amounts of information to manage.

To facilitate information management on such a huge scale Intranet systems have evolved over time. In most cases, so as to increase management capability without wasting existing capability (i.e. without completely replacing existing servers and computers), instead of replacing entire Intranet systems, additional servers and computers are simply added to an existing Intranet network.

While this piecemeal approach to Intranet enhancement minimizes hardware costs, this approach results in an extremely complex system wherein it is often relatively difficult to direct information to known electronic memory locations (i.e. server storage addresses) which are later easily accessible. While such storage addresses could be manually provided, providing such addresses manually is particularly cumbersome as many addresses are complex and difficult to specify. This is because a single facility or related facilities may employ many different servers and each server may have access to several different memory devices. Addressing schemes have been further exacerbated by the Internet where there may be several thousand servers and it would be impractical for a user to attempt to manually enter every server address used for storage.

To overcome the addressing problem most Intranet servers are equipped to automatically assign server addresses to specific types of user provided information. To this end, a browser is typically loaded onto each Intranet capable computer which communicates with system servers. When a user contacts a server to interact therewith (i.e. to provide information thereto or receive information therefrom), the server sends instructions to the browser indicating what should be displayed on the computer screen. Typically the screen indicates the server which originated the browser instructions, includes hyperlinks to various related server addresses, includes some instructions on how to use the server via the browser and provides blanks for entering information which is to be returned to the server for storage or processing.

In addition the server provides addresses to displayed hyperlinks and for information which is to be entered by a user. Typically the server provided addresses are held in computer memory and not displayed. After the physician indicates that information has been entered or selects a hyperlink, the browser software transmits the information to the server or contacts the server indicated by the hyperlink address.

Where information is sent to a server, when the server receives information the server may do any of a number of different things including storing the information at a server address or some type of processing and sending additional instructions to the browser. Where a user selects a hyperlink the server indicated by the hyperlink address
responds to the selection by providing a different set of browser instructions for configuring the browser screen.

[0014] For example, in the hospital environment a first browser screen might display several user selectable hyperlinks for entering different types of information into the system and no blanks for entering information. For instance, a first hyperlink may be to a pharmacy server to request a screen presentation to enter pharmacy information, a second link may be to a billing server, a third link may be to a patient history server and a fourth link might be to a prescription server. In this case, to enter information the user first has to select one of the hyperlinks.

[0015] When a hyperlink is selected, the server indicated by the hyperlink address provides instructions to the browser for configuring the browser screen. For example, a server used by a pharmacy may provide instructions to configure a screen including, along with instructions for filling in blanks, a first blank for entry of a patient’s name, a second blank for entry of a physician’s name, a third blank for entry of a dispensed drug and a quantity indicator and a fourth blank for entry of the dispensing date and time.

[0016] After a physician indicates that required information has been provided, the browser transmits the information to the pharmacy server. When the server receives the information it stores or processes the information and then typically returns a message indicating that the information has been stored or processed.

[0017] After a pharmacy record has been stored, when a pharmacist reviews records on the pharmacy server the pharmacist can verify, among other things, that a specific prescription was dispensed, the date and time of dispensing, which patient received the prescription and which physician dispensed the prescription.

[0018] To enter some other type of information such as billing information, using the first screen, a physician might select a second billing server hyperlink. When the second hyperlink is selected, the billing server provides screen configuration instructions and a return target address for information to be returned to the server for storage. The browser displays the billing input screen and waits for the physician to indicate that information has been provided. Thereafter the provided information is transmitted to the server at the server address and is either stored or processed. In this manner all information addressing and control is facilitated by the servers, not the system user.

[0019] While such information receiving and addressing systems can meet the information gathering needs of some facilities, such systems have a number of shortcomings. First, information gathering and entry into such a system is extremely time consuming and therefore is often thought of as an onerous task which is to be avoided. For example, in a medical facility, when a physician makes her rounds, the physician may visit with twenty or more patients, performing examinations and procedures, diagnosing illnesses and prescribing and administering drugs. Each visit requires information gathering related to symptoms, diagnosis, prescription, procedures and examinations performed and drugs prescribed and administered. When this information is gathered via a pen and clipboard, the information must later be entered into the system and stored at a specific and accessible location.

[0020] Most physicians are not particularly adept at data entry. In addition, most physicians are extremely busy and therefore do not have the time to personally enter written information into a system via a browser. For these reasons either information is never entered into a system or a person specifically earmarked for data entry is required. While a data entry person may be expensive, the alternative (i.e. not entering the information into a searchable form) is not acceptable as information must be properly archived.

[0021] Second, even where a data entry person is provided, under the press of time many physician’s have developed their own, personalized shorthand to expedite note taking during patient visits. In addition, often physician’s writing styles are very different making it difficult at best to decipher handwritten records during data entry. Shorthand and sloppy or varying writing styles make data entry by someone other than a physician extremely difficult.

[0022] Third, when information is entered into a system manually by someone other than a physician, the likelihood of mistakes is extremely high due to imperfect translation of handwritten notes, the fact that entry personnel typically are not trained in medical terminology and the fact that many medical terms are very similar, thereby increasing the likelihood that one term may be substituted for another.

[0023] Fourth, because tolerance for errors in medical records is extremely low, there should be some way to force physicians to check the accuracy of system records prior to allowing permanent storage. The present server/browser systems do not require physician approval of records prior to storage. In other words, in many cases a data entry person may enter a physician’s notes and the physician may never check the notes for accuracy.

[0024] Fifth, even when someone other than a physician enters information into a system and a physician intends to revisit the information prior to permanent storage to check accuracy, despite the importance of record review, because of the press of time, record review by physicians is typically low on a physician’s priority list. Where a physician allows even a few days to pass prior to reviewing information for approval, a physician’s recollection of what transpired during a patient visit may not be accurate and information errors may result.

[0025] Sixth, even where a physician takes on the task of entering all information into a system to ensure quality control, the task of moving about from one browser screen to another to input information which is directed to correct server storage locations is onerous where many different records have to be entered and stored. For example, a physician may collect twenty different records while making rounds. Five of the records may have to be stored in patient record’s on a patient’s history server, five records may have to be stored on a pharmacy server, five records may have to be stored on a billing server and the remaining five records may have to be stored on an inventory server. In this case, the physician would have to jump from one browser screen to another during data entry to enter the twenty records into the system. While this simple task might not be objectionable where there are only a few records, clearly, as the number of records which a physician is expected to make increase, the task of jumping among different browser screens becomes more taxing.

[0026] Seventh, in many cases some information may have to be provided to many different servers and therefore might have to be entered by a physician or a data entry person more than once. For example, where a drug is prescribed for a patient drug dispensation and administration information may have to be provided to many different servers for different purposes. A pharmacy server may require an administra-
tion record to ensure that a drug has been delivered, a billing server may require a record of dispensation for billing purposes, a patient record server may have to be updated to indicate that the drug was received, when the drug was received, the quantity of the drug received, the physician who administered the drug and so on, an inventory server may require an administration record to update an inventory list and automatically order drugs to meet anticipated requirements, etc. To provide all of these records to all of the servers, a physician would have to access four different browser screens, a separate browser screen for each server, and duplicative information would have to be entered to be delivered to each server.

[0027] Eighth, typical systems do not make any record of who approved information entered into a system and therefore there is no way to determine if an authorized physician approved a record or some clerical personnel accidentally approved a record before storage.

[0028] Various electronic devices have been developed to aid in the information gathering task. One handy information gathering device is the dictation device (DD) which can be used to record a physician’s audio (i.e. voice) notes during a patient visit. To this end, a typical DD includes a processor, a memory (typically an electronic memory), a microphone, a speaker and some type of activation button. To take audio notes a physician positions the activation button in a record position and speaks into the microphone, the processor recording all voice notes in the memory. DDs often also allow audio review of oral notes and re-recording features to correct mistakes.

[0029] In facilities where physicians regularly use DDs, recorded notes are provided to data entry personnel who manually type audio recordings into an Intranet computer terminal for storage on a server. In the alternative, recently some software has been developed which can automatically convert audio recordings into text files for digital storage.

[0030] While DDs are preferred by some physicians, DDs do not overcome many of the shortcomings of manual (i.e. pen and paper) record keeping which are discussed above. For example, unless a system includes voice recognition software, data entry personnel are still required, physician shorthand causes transcription problems for both a data entry person and transcription software, mistakes may be made during transcription due to imperfect dictation and complex medical terminology, there is no procedure to ensure that information accuracy is checked or to indicate who approved information prior to permanent storage and it takes a large amount of time to enter information into the system.

[0031] Another handy information gathering device is a hand held device (HHD) which streams the information gathering process and the process of entering information into an Intranet system. To this end, a typical HHD may include a keyboard or the like, a processor, a memory and a transmitter. The board takes the place of a conventional clip board and is used to manually and remotely enter information which the processor stores in the memory. After information has been entered via an HHD, to provide the information to the system, the HHD transmitter is positioned in close proximity to a computer input device and the information is transmitted to the input device via a message including a series of signals.

[0032] To intelligibly receive a transmitted message and provide information contained therein to a browser for ultimate delivery to a server for storage or processing, a message receiving computer must be capable of translating the transmitted message into the language used by the server which is typically the hypertext markup language (HTML). This task is accomplished in one of two ways. First, the input device may include special dedicated hardware which converts the message into HTML, the hardware resembling a disk drive in the way it interacts with a browser. Second, the input device may simply provide the received message to the computer processor and software loaded onto the processor might be designed to translate the message into HTML.

[0033] Thus, HHDs can be used to eliminate physician’s hand written notes thereby streamlining the data gathering/entry process. In addition, as a physician enters information into an HHD, the physician can approve entered information immediately eliminating the need to later revisit the information for approval.

[0034] While HHD technology goes a long way to solving many of the problems associated with remote information gathering, problems still exist. First, it is likely that physicians will object to having to manually enter information into an HHD for the same reasons that physicians object to entering information into regular computer terminals. In addition, with an HHD information entry is even more objectionable because most HHD keyboards are relatively small.

[0035] Second, patient’s will likely object when they perceive that a physician’s time during a visit is split between the patient and an HHD for information entry. This is particularly true in the case where it might be difficult to enter information into the HHD thereby requiring additional data entry time.

[0036] Third, even if there were some quick way to enter information into an HHD, transmission of the information from the HHD to a browser and ultimately to a server for storage or processing is a relatively complex task. For example, assuming five records are stored in an HHD for transmission to a browser and that each of the five records is different such that each record ultimately has to be stored on a different server. In this case, prior to transmitting each record to the browser, the physician would have to select the proper browser screen for data transmission. For example, if the first record is to be stored on a pharmacy server, the physician has to select the pharmacy browser screen prior to transmitting the first record. After the first record is transmitted to the browser the browser then provides the record to the pharmacy server which is associated with the screen. Next, assuming the second record is to be stored on the a billing server, the physician has to select the billing browser screen prior to transmitting the second record. After the second record is transmitted the browser provides the record to the billing server. Not only is this process cumbersome, but the HHD would have to have some mechanism which indicated to the physician which record is queued up for transmission so that the physician could select the proper browser screen and associated server address.

[0037] Fourth, conventional HHDs do not indicate who approved a record for ultimate storage.

[0038] Fifth, again, where duplicative information must be provided to several different servers, a physician has to separately select a browser screen associated with each server and transmit the information to be stored once for each server which is to receive the information. This is time consuming and therefore objectionable.

[0039] Some HHDs have been designed to facilitate a pseudo-addressing scheme whereby an ultimate server target address can be selected for some specific types of HHD
information. For example, some HHDs allow a user to enter an E-mail address for a message to be delivered via an Intranet or Internet system.

[0040] At first blush an HHD which specifies a pseudo-address appears to overcome many of the problems associated with transferring information from an HHD to a server for ultimate storage. Thus, if server addresses can be specified, a single generic browser screen can be used as an intermediary between an HHD and servers, the HHD, not the servers, specifying where HHD information should ultimately be delivered for storage or processing.

[0041] Unfortunately, instead of simplifying the information management task, pseudo-address specifying HHDs add a new wrinkle of complexity to a browser system. To this end, while existing address specifying HHDs can provide both information (i.e. a message in the case of E-mail) and an ultimate target address, a dedicated “clearing house” server is required for a number of purposes. First, because the HHD cannot specify configuration of a browser screen, a clearing house server is required for screen configuration.

[0042] Second, because Intranet addresses are often extremely complex and difficult to manually specify, to simplify address specification, HHD provided addresses usually take a short hand form which in and of itself cannot be used by a browser to direct information to a specific server. The short hand address is provided to the clearing house server via the browser. Therefore, the clearing house server uses the short hand address to formulate a more detailed target address specifying a different server for message delivery. Thus, the clearing house server must have some clearing house software for processing received information.

[0043] Third, in addition to providing browser screen configuration information, the clearing house server also has to specify the clearing house server address so that HHD information and the short hand target address are provided to the clearing house server for further distribution.

[0044] In short, even where an HHD can provide a pseudo-address for targeting information, a dedicated clearing house server with special processing software is required.

[0045] To appreciate the added wrinkle of complexity in systems which facilitate pseudo-address specification, consider an exemplary system including HHDs which can specify E-mail messages and associated pseudo-addresses. In this case, to provide an E-mail message to an Intranet, an HHD user must first select an E-mail browser screen via a computer. When the E-mail screen is selected, the computer communicates with an associated E-mail server which provides information to the browser including screen configuration information and the E-mail server address. The browser thereafter displays a properly configured screen for receiving information from the HHD.

[0046] Next, the HHD user positions the HHD in close proximity to a computer input device and transmits the E-mail message, including E-mail address, to the browser. The device provides the message and E-mail address to the browser which in turn transmits the message and E-mail address to the E-mail server specified by the server address associated with the screen. When the E-mail server receives the message and E-mail address, the E-mail server uses the E-mail address to form a relatively more complex address specifying the target for the E-mail message and then transmits the E-mail message to the more complex address and intended recipient. Clearly this system is more complex than a typical Intranet system as a dedicated clearing house server is required for both screen configuration and additional processing.

[0047] One advantage of conventional paper type reporting systems is that original documents can be authenticated simply via a personal signature. Thus, to determine authenticity an original document can be located and a signature examined.

[0048] Unfortunately, often original documents cannot be located for authentication. Because copies are easy to manipulate (e.g. signature cut and paste and general information modification), document copies usually cannot be relied upon for verification of their content. Usually, the only reason copies are relied upon is because original documents cannot be retrieved.

[0049] Document authentication problems are further exacerbated in the digital realm as document modification and signature picture cutting and pasting is relatively easy using standard computer functions. Thus, for example, where a document is transmitted from one computer to another and includes some type of signature picture, it would be advantageous to have some way to authenticate the content of the received document.

[0050] One solution to this authentication problem is described in U.S. Pat. No. 5,689,567 (the “’567 patent”) which is entitled “Electronic Signature Method and Apparatus,” which issued on Nov. 18, 1997. In the ’567 patent, to enable document authentication of a digitally stored document which is subsequently accessed, prior to storing the document, a digital signature picture is encrypted as a function of the document content and is further encrypted as a function of a private (i.e. secret) key. The encrypted signature picture and document are stored.

[0051] Thereafter, when the document is reaccessed, the signature picture is decrypted using a public key and as a function of the document content thereby generating the document including a signature picture. Where the document is authentic, the resulting signature picture matches the original signature picture. Authentication is performed by visually comparing the resulting signature picture to the original signature picture.

[0052] While the ’567 patent invention is useful, the ’567 invention has a number of shortcomings. First, after a document is retrieved and decrypted, often it will be useful to store the document in a more accessible form such as in the form of a conventional word processor document, spread sheet, etc. In this case, after the initial decryption, there is essentially no way to subsequently authenticate a document. Thus, for instance, after a word processor document is generated and stored in decrypted or plain text form, the document may not again be accessed for a long time (e.g. years). The next time the document is accessed, because of the passage of time, it may be desirable to re-authenticate. The ’567 reference does not facilitate re-authentication.

[0053] Second, it is often advantageous to generate a hard copy (i.e. paper) of a digital document for more conventional storage or conveyance to another party. Again, the ’567 patent facilitates a first authentication by visual comparison but thereafter authentication is impossible. For example, after a paper document with a digital signature picture is generated, the paper document may be stored in a conventional binder-type file for a long time (e.g. 5 years). Thereafter, the paper document may be retrieved for review. When retrieved there is no way to authenticate the document. This problem is
exacerbated by the fact that many documents are copied and copies of documents are copied and, as with an original paper document which is digitally signed there is no way to authenticate a copy.

Thus, it would be advantageous to have an information gathering system for remotely gathering information, reviewing and approving information, identifying who generated information and identifying who approved information prior to storing the information. In addition, it would be advantageous if such a system facilitated easy downloading of the information from an information gathering device to a browser for ultimate transmission to a server for storage or processing. Moreover, it would be advantageous if such a system could be used with a conventional Intranet and did not require a dedicated clearing house server or specialized server software. Furthermore, it would be advantageous to have a system which can authenticate either a hard copy or a digitally stored document by simply analyzing information provided on the document.

BRIEF SUMMARY OF THE INVENTION

The present invention relates to an information gathering system wherein an information collecting device (ICD) is equipped to remotely, automatically and electronically collect a large portion of the information that a physician may be required to provide during each of several different patient visits, information related to each visit forming a separate information unit. The ICD includes a processor, a transceiver and a memory. The ICD is to be used with other “smart” devices in a medical facility to collect information which describes facility events.

For example, one smart device may be an IV pump which includes a processor, a memory and a transceiver. During a patient’s stay in a facility, the IV pump is connected to the patient, the pump processor monitors all pump activity including type and amount of fluid dispensed and time of administration. Information collected by the pump is assembled into an information segment. When a physician visits the patient, the pump processor transmits the information segment to the physician’s ICD.

Another smart device may include a medical container which includes an electronically locking lid, the lid includes a processor, a memory and a transceiver. In one example, a drug may be dispensed by a facility pharmacy into the container. A pharmacy computer provides administration information including the type and amount of drug dispensed, the patient for whom the drug is dispensed, the time period in which the drug should be administered and perhaps the physicians who are authorized to administer the drug. All of the administration information is stored in the container memory. When the container is opened, the container identifies the time and date. The administration information and opening time and date are assembled into an information segment. Then, after drug administration, the physician causes the container processor to transmit the information segment to the ICD processor for storage in the processor memory.

Yet another smart device may include a patient identification bracelet which includes a processor, a memory and a transmitter. Patient identifying information is stored in the bracelet memory as an information segment. When a physician visits a patient, the physician causes the identification bracelet to transmit the information segment which identifies the patient. The transmitted information segment is received by the ICD and stored as part of a collected information unit.

When several different information segments are received by the ICD during a single patient visit, the ICD may assemble one or several different information units from the segments, each information unit including at least one and possibly several information segments.

One object of the invention is to reduce the amount of manual data entry and simplify information management. To this end the inventive ICD facilitates automatic electronic retrieval of data gathered by smart devices including diagnostic and monitoring devices, electronic lock-lid containers, IV’s, blood samples, etc. Moreover, the ICD may also facilitate automatic patient identification. Furthermore, the ICD processor may provide a time and date stamp indicating when an event which is related to an information segment occurred.

In addition, the ICD processor may also provide other information in information segment form which is appended to other information segments to form information units. For example, in a preferred embodiment the ICD also includes physician identifying information in its memory which an ICD appends as an additional information segment to information units. This feature further reduces the amount of manual record keeping required.

When an information unit is assembled by the ICD processor, the ICD processor provides a complete target server address for the information unit which is appended thereto to form an information packet. The information packets are transferred to an Intranet system for review, approval, modification and eventual storage at the specified target addresses.

An Intranet system which is suitable for use with the inventive ICD includes at least one and preferably several computer terminals, a plurality of network devices (i.e., memory storage devices or servers) and a network of information busses which links the computers to the network devices. An Intranet browser is loaded onto each of the computers. In addition, each computer includes a processor, a memory and some type of input device for receiving information packets from ICDs.

The computer processor receives information packets via the input device from the ICD, identifies the separate packet sections including the information units and associated target addresses, and stores associated units and addresses together in the computer memory for subsequent retrieval. Thereafter, the browser allows a physician to review and approve each information unit for delivery to a server identified by the target address. The browser may also allow a physician to edit information units or reject information units.

When a physician elects to approve an information unit, the browser sends the approved information unit to the associated target address (i.e. the target address specified by the ICD).

Another object of the invention is to provide an ICD which provides server addresses for information units. To this end the inventive ICD can generate server target addresses in any of several different ways. First, the ICD processor may receive the target address from a smart device via the ICD transceiver. For example, in addition to indicating the information indicated above, a smart medical container may also indicate a target address for associated information segments. For instance, the target address may indicate a pharmacy server address. When the ICD receives the target address the ICD appends the target address as a target address segment to
the information unit in the information packet which is thereafter transferred to the browser.

[0067] Second, the ICD may receive a command from a user indicating a target address. To this end, while target server addresses are generally too long to manually enter into an ICD, where a facility only routinely uses a handful of servers, the ICD may be programmed so that each distinct server address is related to a separate address specifying task identifier in the form of an ICD button. For example, where a facility only uses five servers including a pharmacy server, a billing server, a patient records server, an inventory server, and a physician records server, an ICD may be designed to have five separate buttons, each of which are uniquely emarked to correspond to a server unique address (i.e. button 1 corresponds to the pharmacy server address, button 2 corresponds to the billing server address, and so on). Then, when an ICD receives an information unit, a physician can select one of the five buttons to indicate a desired server to receive the information unit. When a button is selected the associated server address is specified by the processor as the target address for a constructed information packet, the target address forms a target address segment and the target address segment is appended to the information unit forming the information packet to be provided to the browser.

[0068] Third, the ICD may be able to formulate a target address based on information received during information collection. To this end, when an information segment is collected, the ICD may automatically identify the general nature of the collected segment from which a proper server address can be surmised. For example, all information segments received from medical containers may have to be provided to a pharmacy server for review by a pharmacist. In this case, when an ICD receives an information segment from a medical container, the ICD can recognize the received information and identify the pharmacy server address as the target address. Thereafter, the ICD forms an information unit including the information segment from the container and perhaps other information (i.e. information from other received segments or information generated by the ICD) and assembles the information unit and target address into an information packet for transfer to the browser.

[0069] As another example, an ICD may be equipped to receive dictation when an activation button is pressed. In this case, the ICD may automatically identify received audio dictation as information to be provided to a transcription pool. Thus, the ICD automatically specifies a transcription pool server address so that digitally recorded dictation can be directed to a transcription server when downloaded to the Internet.

[0070] In addition to providing a complete server address to a browser, the inventive ICD also provides complete browser screen configuration information which is required to configure a browser screen for displaying information unit information. The configuration information is provided in a configuration segment which is appended to the information unit and the target address. Hereinafter, unless specified otherwise, an information unit will refer to all information in an information packet except the target address segment and configuration segment.

[0071] Having an ICD which provides specific server addresses and browser configuration information is advantageous for a number of reasons. First, an address and configuration specifying ICD facilitates easy information transmission from the ICD to a browser and ultimately to desired servers for storage. Because the inventive ICD provides server addresses and browser screen configuration information, a generic browser can be employed to receive any information which is to be transmitted to any server. In other words, no information from a server or server processing is required to transmit ICD information units to target addresses (e.g. no clearing house server is required). Thus, any ICD information packet can be provided to a generic browser, the browser configuring the screen in accordance with the configuration segment information, displaying information unit information and storing the address specified by the target address segment for ultimate delivery of the information unit after approval. In effect, the ICD performs all of the front end tasks (i.e. tasks prior to permanent information storage) which are typically reserved for a browser and eliminates the need for clearing house processing.

[0072] Second, target address specification can be used to facilitate quality control. For example, when a drug is dispensed into a smart medical container as described above, the administration information can be provided by a pharmacy server (i.e. a specifier apparatus) upon dispensation. Among other things, the administration information can specify a target address on the pharmacy server for a subsequent information packet describing the administration event including time, date, patient, physician administering, amount and so on. When the container is opened, the container transmits the administration information in the form of an information segment to the ICD which assembles an information packet including the target address in the target address segment. Subsequently the packet is transmitted to the browser and, after approval, the information unit is transmitted to the target address which specifies the pharmacy server.

[0073] Advantages related to this loop closure possibility include the ability to track drug administration. Because the administration information originated with the pharmacy server and the information unit was returned to the pharmacy server, the pharmacy server can determine if all prescribed drugs and the proper doses have been administered at the right times to the right patients by authorized physicians.

[0074] Another advantage from loop closure is the ability to provide servers which automatically generate quality control reports. Servers which can close an information loop can be programmed to indicate all successful administrations, administrations which were underway but not during prescribed times, included other than a prescribed dose or other than a prescribed drug, were administered by other than an authorized physician, etc.) and administrations which were missed.

[0075] According to another aspect of the invention is an ICD may be programmed to provide more than one target address for a specific information unit. For example, where an information unit includes drug administration information, the unit may be required by each of a pharmacy, a billing department and an inventory department. In this case, whenever an information unit includes drug administration information, the ICD provides three target addresses including addresses specifying each of a pharmacy server, a billing server and an inventory server.

[0076] Thus, another object of the invention is to simplify the process of providing duplicative information to several different servers by enabling specification of several servers at one time.

[0077] In all cases the present invention contemplates that, prior to transmitting information packets to a browser, a phy-
sician must first log onto a computer via some procedure which identifies the physician and verifies that the physician is authorized to enter information packets into the browser or is authorized to approve information units prior to permanent storage. This log-on procedure may be as simple as, in the case where the physician’s ICD includes physician identifying information, transmitting the physician identifying information to a computer terminal via the computer input device, the computer processor thereafter performing a verification process. In cases where a physician’s ICD does not include physician identifying information, a more traditional log-on procedure may be required wherein the physician enters a password which identifies the physician. In any case, the invention also contemplates a system wherein, when a physician logs onto a computer and transmits information packets to the computer browser for review, editing and approval, after approval, the computer includes what amounts to a digital signature in the information unit prior to storage at the target address. The digital signature is generated from the log-on information and identifies the physician who edited and approved the information.

[0078] Thus, another object of the invention is to provide a system wherein, prior to storing an information unit on a server, a physician reviews the information unit to affirmatively determine the accuracy of the unit and assures accuracy through her digital signature.

[0079] While a digital signature may be relatively simple, taking the form of a graphical representation of the physician’s signed signature (hereinafter “signature picture”) which is appended to a document, the present invention also contemplates a “watermarked” signature picture wherein the watermark varies as a function of the content of the document to which the signature picture is appended. This type of watermarked signature picture facilitates subsequent signature picture authentication as well as document authentication. For example, after a document is generated, to check authenticity the watermark may be examined to, in effect, recreate the document content to determine if the signature picture was authentic.

[0080] One other object of the invention is to facilitate secure digital signatures which cannot be electronically copied from one document to another without detection. This is accomplished by providing document specific watermarked signatures.

[0081] Another aspect of the invention allows a browser to store information units on a dedicated server or on a computer hard drive for later review and approval. In this case, after an information unit is stored, at some later time, a physician may reaccess the information unit for editing and approval.

[0082] Thus, another object is to facilitate semi-permanent information unit storage for a reasonable amount of time so that a physician can approve or edit information units when convenient.

[0083] A related object of the claimed invention is to minimize the amount of training necessary to implement a comprehensive data collection, data security, and data management system for hospital and patient records. The inventive ICD and associated system is extremely simple to use for both information collection and review. In its simplest form collection amounts to causing smart devices to transmit collected information. Transfer to a browser for review amounts to causing an ICD to transmit all assembled information packets. Review amounts to using a single browser screen and a few commands to edit and then approve of information units after which units are automatically stored.

[0084] Yet another concern is to, where possible, minimize time between data collection and data approval to cut down on errors attributable to faulty memory. Even a few days between data collection and approval can cause information errors. To this end, because the inventive ICD system is simple to use and information downloading is extremely easy, the review and approval process is appreciably short circuited.

[0085] Another object is to, where possible, provide information in a standard format so that virtually all commonly trained physicians can glean identical information from gathered information. To this end, information provided by smart devices is always provided in a specific format and is stored in a similarly specific format.

[0086] According to another aspect of the invention the ICD may be provided with some other type of input device so that a physician can specify non-standard information for recordation. For example, a physician may identify a new and unexpected symptom which should be recorded and which is not indicated by a smart device. In this case, the ICD may include either a small keyboard or a dictation means for entering other information to be recorded.

[0087] Thus, another object of the invention is to, while providing a system which automatically generates much of the information required to be collected by a physician, allows the physician to record other information which should be recorded but is not automatically provided by the system.

[0088] One other problem with conventional information systems used in hospitals and other facilities which require large amounts of remote data gathering is that, besides a simple password interrogation system, in most cases nothing else stops an unscrupulous person from accessing a facility computer system to examine, add or modify information stored on the system. In fact, where an authorized person logs onto a terminal and leaves the terminal momentarily, another person could easily access the terminal and system information via the terminal under the guise of the authorized person.

[0089] The present invention overcomes this terminal security problem in several different ways including an identification system which ensures that a person who logs onto a system is authorized. To this end, in one embodiment, a person’s ICD includes some type of body indicia identifier which can be used to identify an ICD user. For example, the indicia identifier may be a finger print reader which compares a users print to an ICD owners print. Where the ICD recognizes a user, the ICD participates in an interrogation by a proximate terminal to gain access to the terminal. Where the ICD fails to recognize the user, the ICD does not participate in an interrogation and therefore access to the network is blocked.

[0090] This indicia identifier concept has many applications outside the ICD art. For example, such an identifier could be placed on a credit card. In this case, when a user is identified, the card could enable a single charge to be made via the card. Thereafter, to make another charge the user would again have to present the user’s print to the identifier to authenticate the user.

[0091] The inventive identifier has several advantages over prior art indicia identification systems. First, because the inventive identifier is personal to a single user, the identifier’s memory need only store finger print characteristics for a single user. For this reason minimal memory is required. In
addition because only one print has to be interrogated, a relatively simple processor can be used to interrogate a finger print and identify a user.

[0092] Second, the inventive identifier keeps personal information secret while still facilitating user identification. In many conventional person interrogating systems which identify body indicia a person's body indicia has to be "given up" to an interrogation system which is not controlled by the person. For example, to enter a building, an interrogation system may require a person to place her thumb on a finger print reader which identifies her print characteristic and then compares her characteristic to characteristics of prints associated with all people who are authorized to enter the facility. In this case the person's print would have previously had to have been provided to the system so that a comparison could be made. Providing personal indicia is viewed as intrusive by many persons and therefore is objectionable.

[0093] With one embodiment of the inventive indicia identifier, all indicia identification occurs on a device (i.e. ICD, credit card) which is controlled by the device owner at all times and therefore control of personal indicia is never forfeited. With another embodiment of the invention a person's indicia is provided to an external interrogation system only for interrogation purposes and is thereafter erased from the systems memory. According to this embodiment, for example, a person's fingerprint characteristics may be stored in an ICD memory, smart card or the like. To gain access to a computer network via terminal an interrogation must occur. To this end, an interrogation system includes a processor which can receive information from the ICD or smart card and which is linked to a print reader. During an interrogating process the person first enables print characteristic transfer from the ICD or card to the processor. Next the person places her thumb on the print reader which provides print characteristics to the processor. Thereafter the processor compares the prints (i.e. from the reader and the ICD or card) and allows access where the prints are identical but blocks access where the prints are different. Then the processor erases the prints from memory and may indicate so for the user's peace of mind.

[0094] The invention also includes a method and apparatus for checking authenticity of a digital or hardcopy document using only content provided on the document. To this end, assuming a document exists in a computer memory and can be displayed for approval on a computer display, a user may examine the document and, if the user approves the document, the user may indicate approval (e.g. via a key or icon selection). When approval is given, the computer performs two tasks. First, the computer provides some form of user or personal identifier to the document in a designated approval field or space. The identifier may take any of several different forms but preferably is a signature picture of the person who approved the document. This first task results in a "signed" document. Second, the computer uses the signed document content (i.e. the original document plus the signature picture) and uses a personal key which belongs to the approver to compute encryption codes, hash code, etc. The encryption code is then used to modify a standard water mark resulting in a watermark which is indicative of the signed document content. The watermark is appended to the signed document. When the document is stored or printed the watermark is included therewith.

[0095] Subsequently, to authenticate the content and signature of the document, the watermark can be read from the document and decrypted using a public key which belongs to the person whose signature appears on the document (supposedly the original approver). At the end of the decryption process, the resulting document should match the signed document and can be compared either visually or automatically to authenticate the signature and the document content.

[0096] These and other objects, advantages and aspects of the invention will become apparent from the following description. In the description, reference is made to the accompanying drawings which form a part hereof, and in which there is shown a preferred embodiment of the invention. Such embodiment does not necessarily represent the full scope of the invention and reference is made therefor, to the claims herein for interpreting the scope of the invention.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0097] FIG. 1 is a perspective view of a security badge capable of communicating with computer terminals and a plurality of smart devices;

[0098] FIG. 2 is a perspective view of a wrist bracelet to be worn by patients or other persons to provide identification through wireless communication with security badges or other smart devices;

[0099] FIG. 3 is a plan view of a computer terminal or workstation being operated by a system user where access is conditioned upon communications between the security badge and the computer terminal;

[0100] FIG. 4 is a plan view of a hospital patient room equipped with a variety of computerized monitoring, treatment, and information devices;

[0101] FIG. 5 is a perspective view of a medical container equipped with an electromechanical locking device controlled by communications through transceiver components;

[0102] FIG. 6 is a block diagram of various electrical components which are incorporated within an exemplary ICD;

[0103] FIG. 7 is a block diagram of a computer network according to the present invention, including a plurality of workstations and databases for data record retrieval and storage and a security verification system;

[0104] FIG. 8 presents the base memory contents of a security badge;

[0105] FIG. 9 presents the contents of the information transferred from a wrist bracelet according to the present invention to a security badge;

[0106] FIG. 10 presents the contents of the information transferred from a medical container according to the present invention to a security badge;

[0107] FIG. 11 presents the contents of a digital message record incorporating a dictated message and other information corresponding to the dictated message;

[0108] FIG. 12 is a list of information transferred from a patient monitoring or therapeutic device to a security badge;

[0109] FIG. 13A is a textual representation of a URL address of medical dispensation record formed in part from the patient's identification number and a time stamp;

[0110] FIG. 13B is a graphical representation of a medical dispensation record with HTML codes for displaying the information in a network browser;

[0111] FIG. 13C is a graphical representation of the record of FIG. 13B as it would be viewed by a system user through a network browser;
Detaile description of the Invention

The present invention may be adapted for use in a wide variety of applications and is suitable for any environment in which numerous data records having one or multiple forms and/or formats are to be collected, stored, archived, retrieved, or translated. By way of illustration and not by way of limitation, unless indicated otherwise, the preferred embodiment is presented in the context of a medical facility environment in which typically there are numerous computer systems in use by various physicians (e.g., doctors, nurses, administrators, etc.), in several related hospitals, and each physician often desires to have access to patient records created by that physician or by other physicians who practice at one of the related hospitals. Throughout this specification, identical numbers represent similar components and symbols.
a physician (e.g., through selection of a hyperlink or entry via device 105), a target server address for reception of the information is provided.

[0137] The target server address will typically take one of two basic forms. First, the target address may simply indicate a database address on one of data bases 158-162 for storing received information. Second, the target address may specify a specific system 194 server and, when a server receives information, the server may determine how to proceed (i.e. process or store the received information).

[0138] Input device 64 is a transceiver which is capable of two-way communication with other devices described hereinafter. While device 64 may be equipped for wired communication, preferably, device 64 is capable of any of several different types of wireless communication. Because of its low cost, energy efficiency, minimally regulated status, and standardization by the Infrared Data Association (IrDA), infrared transmitter and receiver components supporting serial infrared communications links comprise the preferred transceiver 194. A variety of infrared communications devices, such as Hewlett Packard's HSDL-1001 transceiver components, may be used to implement the preferred communication means. Alternatively, other communication means (e.g. acoustic, radio frequency, or electromagnetic coupling) may be supported.

[0139] Referring to FIGS. 3 and 7, dispenser 150 may take any of several different forms but preferably is a terminal like terminal 60 including a processor 107, a keyboard 115, a memory 101, a speaker 110, or a microphone 22 and an indicator 111. In addition, other useful functionality is provided by processor 107, for example, timing, counting, indicator and display control and so on. Dispenser 150 is in communication with pharmacy server 186. Thus, server 186 provides screen configuration information as well as server target addresses to dispenser 150 for interaction with a pharmacist who is responsible for dispensing drugs. In addition to dispensing drugs, dispenser 150 may also dispense target address information and browse configuration information to other system devices used for remote information collection and may perform some information tracking tasks described in more detail below.

[0140] In addition to the devices, systems, and servers identified above, the inventive system includes a series of other electronic devices which cooperate to remotely gather information within a medical facility and provide information to system 194 for storage and manipulation.

[0141] Referring to FIG. 1, a mobile information collecting device (ICD) is illustrated in one embodiment as a security badge 10 which may be clipped to a physician’s clothing or worn by chain around a physician’s neck. While this embodiment implements the invention in the context of an identification badge, the invention could be instantiated in other shapes, such as a ring, a personalized pointing device or a small hand held computer. In keeping with its preferred resemblance to a typical identification badge, ICD 10 is affixed with identification text (e.g., a receiver/transmitter) which operates as both a data collector and an output device, an audible alerting device 20, an activation button 18, a microphone and audio digitizer 22, and a dictation button 26. ICD 10 may also incorporate additional electronic identification means such as a magnetic strip (the general location illustrated at 30) and may also incorporate a small key pad (not illustrated) for entering additional information.

[0142] Referring also to FIG. 6, ICD 10 comprises a processor 250 which is linked to each of a battery 252, a real-time clock 254, a memory element 262, an audible alerting device 20, a transceiver 14, an activation button 18, a microphone 22 and a dictation button 26. Display 16 of ICD 10 may be any of a variety of formats, including but not limited to a photograph, a light emitting diode array, a liquid crystal panel, and an active matrix display. In addition, ICD 10 may include a display 258 such as a light emitting diode array, an LCD screen, or a passive or active matrix screen, which is linked to processor 250.

[0143] Referring to FIG. 8, exemplary information 300 which may be stored in memory element 262 is illustrated. Information 300 includes both “base contents” and “optional information”. The base contents comprises the minimum information which should be stored in a personalized ICD such as identification ICD 10 and includes a physician’s password or private/public digital security key information which can be used to log onto a computer terminal to provide information to, or review information thereon. The optional information includes other information which is descriptive of a badge owner including a user identifier such as a name, identification number, occupation, privileges and so on.

[0144] While personalized ICDs are preferred, the invention also contemplates other types of ICDs which are not personalized and can therefore be used by any facility personnel to collect information for entry into a facility computer system. In this case, however, prior to entering information into the system, it is contemplated that a physician would log on to a computer terminal in a more conventional manner via system 168 which would identify the physician for security purposes. For example, the physician might manually enter a personal identification number to gain access to the computer terminal for information entry and retrieval.

[0145] ICD 10 is to be used with a plurality of different “smart devices” for remotely collecting information. In addition to remotely collecting information, inventive ICD 10 is equipped to provide information packets to terminal input devices 64 which are formatted and addressed according to uniform standards in order to minimize the need for human intervention in categorizing and archiving patient records. Information packets are formatted and addressed according to conventions, such as Java or a markup language supporting interactive display by browser 115. While any standard format (e.g. HTML, Java . . . ) may be supported and it is contemplated that the present invention may be used with any computer language format, hereinafter, in the interest of simplifying this explanation, the invention will be described with reference to the HTML format only.

[0146] By formatting information packets in HTML format a receiving computer terminal 60 does not need additional programming or input to display or manipulate information in an information packet. In a preferred embodiment, formatting and addressing of information packets is done partially or entirely by ICD 10 itself, using time stamps, patient identification information, and the information or contents 300 (FIG. 8) incorporated in memory element 262 (FIG. 6) of ICD 10. In this manner all the information required to display information packet information and to send the information to an appropriate database or server is included in the information packet transferred from ICD 10. An exemplary information packet is described in more detail below.
Referring to FIG. 19, an exemplary smart device 75 generally includes a processor 77, a memory 79 linked to processor 77 and either a transmitter or a transceiver 81 (i.e. a receiver/transmitter). In addition, each smart device 75 may also include one or more activation buttons 83, some type of indicator (e.g. a light 85 or audible alarm in the form of a speaker 87) and a display 88. Smart devices like device 75 collect, generate, and/or are provided information which is assembled into information segments to be transmitted to ICD 10 for collection. Many smart devices 75 are contemplated by the present invention, however, in the interest of simplifying this explanation, only a small number of smart devices are described. Hereinafter when specific smart device components are referenced, the specific components will be referenced by the same numbers used in FIG. 19 followed by one or more “†” indicating components associated with specific devices as described hereinafter.

Referring now to FIG. 2, one smart device is a patient identification bracelet 40. An exemplary bracelet 40 is described in U.S. patent application Ser. No. 09/007,290, which is entitled “Identification Bracelet With Electronic Information”, now U.S. Pat. No. 5,883,576, which was filed by the present inventor and is incorporated herein by reference. Bracelet 40 includes a flexible and extendable band 44, a securing clasp 48, a processing device 75† and a wireless communication means in the form of transceiver 81†. Bracelet 40 is similar to existing bracelets used to identify patients in hospitals, with the exception of the processing device 75† which includes transceiver 81†. Textual information (not illustrated) is typically affixed to band 44. Transceiver 81† is preferably similar to transceiver 14 of ICD 10 so that transceivers 81† and 14 can communicate back and forth. Like general device 75 (see FIG. 19), device 75† includes a processor and a memory element linked to the processor (not illustrated). Referring also to FIG. 9, exemplary patient identification information 320 to be stored in the memory of device 75† is illustrated and includes, at a minimum, a patient identification number identifying the patient who wears bracelet 40. In addition, the identification information 320 may also include other descriptive information as indicated.

Referring to FIG. 5, another smart device is a medical container 200. U.S. patent Ser. No. 08/955,475, entitled “System And Apparatus For Administering Prescribed Medication To A Patient”, now U.S. Pat. No. 6,032,155, which was filed by the present inventor and is incorporated herein by reference, describes an exemplary medical container. Exemplary container 200, which may be used to transport and provide auditing and limited access for medications, blood or tissue samples, or other inventory, includes a lid 204, a securing latch 232, a latch release button 228, and an electronic identification or processing device 75†. Textual identification 208 may be attached to lid 204. Processing device 75†, like general smart device 75 (see FIG. 19) includes a processor which is linked to a memory, a battery, a transceiver 81†, an activation button 83† and an audible alarming device 87†.

Referring also to FIG. 10, exemplary information 340 which might be stored in the memory associated with processing device 75† is illustrated. Once again the information is divided into a minimum amount of information which should be stored and optional information. In the case of a drug to be administered, the minimum information includes medication name and medication quantity. Optional information may include, among other things, the name of a patient for whom the drug is dispensed, the date and time at which the drug should be administered and the names of physicians authorized to administer the drug. Other information would be provided in the case of a tissue sample, a blood sample, etc.

Referring again to FIG. 5, it is contemplated that latch 232 release may be conditioned on any of a number of different precise sequences of events. The events may include release within a time-window for treatment, the successful exchange of identification information between a physician’s ICD 10 and processing device 75†, the successful exchange of identification information between a patient’s identification bracelet processing device 75† (see FIG. 2) and processing device 75† and the manual depression of the latch release button 228. An example of a lid unlocking sequence is described in more detail below.

Referring to FIG. 4, an exemplary patient room 104 includes a computer terminal 60, a patient bed 88 and various other devices. The other devices include two smart devices including a patient monitor 80 and a patient treatment device 116, each equipped with a wireless transceiver input device 64 which is similar to transceiver 75 on band 40 (see FIG. 2) and transceiver 75 on container 200 (see FIG. 5). Monitor 80 and device 116 are smart devices meaning that each of these devices typically include the components illustrated in FIG. 19 (i.e. in addition to a transceiver, each device includes a processor, a memory, at least one activation button and some type of output device such as an LED or computer screen for visual indication or a speaker for audio indication). In this example, it will be assumed that each of devices 80 and 116 are not hardwired to network 194.

Also shown in FIG. 4 is an optional bedside communication device 96 which is equipped to communicate with wireless transceiver devices 64. Communication device 96 may be connected to an optional patient identification display 100 equipped with wireless transceiver device 64 or to a patient identification display 120 outside of room 104.

II. OPERATION OF A COMPUTER TERMINAL IN ACCESS CONTROL

Generally, it is contemplated that a terminal used with an ICD 10 will be capable of, in addition to facilitating transfer of information packets from the ICD 10 to the terminal, facilitating use of other conventional computing programs (e.g. a word processor, a spread sheet, Internet access, etc.). In enabling access to any facility application, security is extremely important.

In the preferred embodiment, authentication, interrogation and data security will be illustrated through the use of conventional “public key” cryptography, such as that implemented in RSA, though other well-known techniques for authenticating a user and securing transmitted data may be employed. In implementing public key cryptography, the security badges and computer terminals are equipped with “private key rings” of one or more private keys and a “public key ring” of one or more public keys. Depending upon their sophistication and the sensitivity of the information they contain, other smart devices in a medical facility, such as monitoring devices or medical instruments, may also be equipped with cryptographic means. The private keys of each ICD 10 are never transmitted or otherwise made accessible outside the ICD 10. For strong compression, each public and private key would typically be at least 128 bytes long. Today, the preferred implementation for smart card encryption capabilities utilizes the Advanced RISC Microprocessor (ARM), such as the ARM 6, the ARM 710, or a variety of customized...
chips integrating the ARM technology, such as the Mykronics Capstone or VLSI’s VMS 210. A variety of other processors, including the Intel x86 processor, would also be suitable. [0157] FIGS. 15A-15F describe the operation of a computer terminal 60 (FIG. 3) in interrogating, establishing and monitoring access by a physician wearing an ICD 10 (FIG. 1). Access is established by providing a substantially unobstructed signal path between the physical wireless communication means 14 (preferably comprising infrared transmitter and receiver components (see FIG. 1)) of the ICD 10 and the wireless transceiver device 64 of the computer terminal 60. The establishment of an unobstructed signal path is facilitated by having the ICD 10 worn on, or attached to, the front of the physician attempting to log on the computer terminal 60. While it is not necessary that the ICD 10 be worn by or attached to the clothing of the physician, securing the ICD 10 to the physician minimizes the probability that it will be lost by the physician.

[0158] Commencing with FIG. 15A, in step 600 the computer terminal 60 transmits an interrogation signal, which is fashioned from a private key of the security verification system 168 (FIG. 7) of the computer network 194, a large random number, and other identification information unique to the security verification system 168. Provided a substantially unobstructed signal path exists between the wireless transceiver device 64 (FIG. 3) of the computer terminal 60 and the wireless communication means 14 (FIG. 1) of an ICD 10, the ICD 10 will intercept, process, and be operable to return a part of the interrogation signal in a re-encrypted form (according to the operation of the ICD 10 set forth in FIGS. 16A-16F, infra).

[0159] In step 604, the computer terminal 60 waits for a period sufficient to allow an ICD 10 to receive, process, re-encrypt, and re-transmit the interrogation signal. If no return response is received, in step 608 the computer terminal 60 waits for a predetermined period of time and, returning to step 600, transmits another interrogation signal. If a return response is received, in step 612 the format of the return response is evaluated. If the format is unrecognized, in step 608 the computer terminal 60 waits for a predetermined period of time and, returning to step 600, transmits another interrogation signal.

[0160] If a return response of a recognized format is received by the computer terminal 60, in step 616 it is decrypted or authenticated using the public key of the ICD 10 which returned the response. In a public key cryptographic system, encryption with a private key uniquely identifies the physician possessing that key (assuming the private key has not been stolen) because an encrypted message can only be decoded using the public key matching the physician’s private key. Accordingly, the security verification system 168, which stores the public keys of each ICD 10 given access privileges to the computer network, attempts to decrypt the re-encrypted interrogation signal using the public keys it retains.

[0161] There are at least two ways in which the decryption procedure may be carried out. In one procedure, the security verification system 168 attempts to decrypt the response signal, one public key at a time, until either a successful decryption is achieved or all the public keys stored by the security verification system 168 fail. Preferably, however, the identification information will have been appended to the encrypted portion of the return response purporting to identify the ICD 10. The security verification system 168 then attempts to decrypt the return response using the public key corresponding to the appended identification information. A successful decryption identifies the ICD 10 that originated the return response. If the decryption is successful, a verification algorithm is used to compare the decrypted return response to the original, pre-encrypted interrogation signal.

[0162] It would, of course, be possible to program the computer terminal 60 itself to perform some or all the functions of the security verification system 168. A physically separate security verification system 168, however, will safeguard the computer network 194’s private keys and the list of public keys of valid system users, preventing appropriation of the keys by one breaking into the computer terminal 60 itself.

[0163] As an additional precaution, the ICD 10 may be programmed to detect and eject interrogation signals that are short and probabilistically non-random. In other words, if an ICD received one or a series of consecutive interrogation signals which were not recognized as being in a valid form, the ICD 10 would reject the signal and fail to respond. This rejection process would frustrate a cryptanalyst’s attempt to derive an ICD 10’s private key by interrogating the ICD 10 with short messages and intercepting the re-encrypted response. This precaution is especially justified if the ICD 10 is adapted to communicate with devices and computer terminals foreign to the computer network 194 and its security verification system 168. This precaution may also limit the damage that could be imposed were a private key of the security verification system 168 compromised.

[0164] In step 620, if the decryption and verification failed to identify an ICD 10 having access privileges to the computer terminal 60, then the operation proceeds again to step 608, where the computer terminal 60 waits for a predetermined period of time and, returning to step 600, transmits another interrogation signal.

[0165] Because an ICD 10 may be misplaced by or stolen from a physician, additional security measures are warranted. The security verification system 168 may be programmed to require that a physician manually enter a password at the beginning of each day. Alternatively, the system could require manual password entry at random times throughout the day, even while the physician is logged on, flagging possible theft and unauthorized use of the ICD 10 should the proper password not be detected. Further, a switch may be incorporated onto the ICD 10 to force it into a mode requiring password entry. More elaborate means, including voice identification or a fingerprint or retinal scan, could also be incorporated into the ICD 10 or at computer terminals 60 to reinforce such security. One example of a fingerprint interrogating ICD and its advantages is described in detail below. It is to be expected, however, that a physician be dispossessed of an ICD 10, that he or she immediately notify the system security administrator to deactivate the access privileges of the ICD 10.

[0166] Provided an ICD 10 having access privileges to the computer terminal 60 has been identified, in step 624 the security verification system 168 determines whether or not to require the entry of a password to enable log on by the physician. This procedure provides a safeguard should the ICD 10 be stolen, deterring unauthorized log on attempts with the threat that the security verification system 168 will detect the breach and apprehend the violator.

[0167] If password entry is required, then in step 632 the computer terminal 60 prompts the physician for a password. Information that is entered may not only be processed by the
computer terminal 60, but also transmitted to the ICD 10 in
encrypted form in order to reset a flag maintained by the ICD
10 indicating that password entry is required. In step 636, the
password is analyzed. If the wrong password has been
entered, in step 640 a counter is incremented. If the wrong
password was entered less than three consecutive times (step
640), the security verification system 168 returns to step 632
and again prompts the physician to enter the password. After
three failed attempts (step 640), however, in step 644, the
security verification system 168 disables recognition of the
ICD 10, records the location of the failed attempt, and notifies
the system administration to alert it to a possible attempted
breach of the system. Other processes may be performed in
the event of a failed interrogation. For example, where data is
to be provided to a terminal after a successful interrogation,
the terminal may block reception of transmitted data after a
failed interrogation or series of interrogations.

[0168] If within the first three attempts, the correct pass-
word is entered, the operation advances to step 648, logging
the physician onto the computer terminal 60 and providing
access to program features and databases in accordance with
the access privileges of physician. In step 652, the computer
terminal queries the ICD 10 for the existence of data records
to transfer to the computer network 194 and causes the ICD
10 to transmit them, if any, to the computer terminal 60 for
database storage, in accordance with the operation detailed in
FIGS. 16A-16F. This query for data records or information
packets may be automatic or may simply be a function which
periodically queries for records as described in more detail
below.

[0169] After completion of the data transfer by the ICD 10
to the computer terminal 60 or, in the event no data is trans-
ferred but another terminal application (e.g. a word pro-
cessor) is employed by the physician, if warranted, the computer
terminal 60 will continue to periodically poll the ICD 10 with
recommitment signals. These recommitment signals may be
specifically addressed to the physician’s ICD 10 and may
incorporate a different random number with each polling.
Further, these recommitment signals may be encrypted with
the ICD 10’s public key stored by the security verification
system 168, instead of or in addition to encryption by the
security verification system’s private key, so that they may
only be intelligibly decrypted by the ICD 10 itself, using its
own exclusively-guarded private key. By periodically polling
the ICD 10, the user input and output devices of the computer
terminal 60, including the monitor, keyboard, and mouse, can
be disabled if the computer terminal ceases receiving
response signals from the ICD 10. A physician may also be
automatically logged out by means of periodic polling.

[0170] This process of periodic polling is illustrated in
steps 656 through 692 of FIGS. 15C-15E. The computer
terminal waits for a predetermined interval in step 656, trans-
mitting a recommitment signal as in step 660, and probes for
a response signal in step 664. If there is a recommitment
response signal, in step 668 its content is evaluated. If the
content of the recommitment response signal is accepted, the
operation proceeds to step 696, discussed infra. If either there
is no recommitment response signal in step 664, or if the
content of the recommitment response signal is rejected in
step 668, an idle/invalid link counter (not illustrated) main-
tained by the security verification system 168 and whose
initial value relative to the log on event was zero, is incre-
mented in step 672.

[0171] The idle/invalid link counter permits the physician
to temporarily turn away from the transceiver device 64 of the
computer terminal 60 or to otherwise interfere with the signal
path. However, if the computer terminal 60 does not receive a
recommitment response signal after several requests, the dis-
play of the computer terminal 60 is blanked, input from any
keyboard or pointing device may be ignored, and other pro-
cessing activities may be suspended. The computer terminal
60, however, continues to transmit recommitment signals.
Should the physician’s ICD 10 respond within a second
period of time, the display will be restored to its previous
condition and the keyboard, pointing device, and processor
will resume normal operation. If the ICD 10, however, does
not transmit a correct recommitment response signal during
the second period of time, the physician is automatically
logged off the computer network 194. When the user is
logged off the computer system, a software program may also
be used to remove any temporary files that have been stored
on disk or in RAM memory, e.g. the cache file used by the
network browser program. Furthermore, access by the com-
puter terminal 60 to the computer network 194 may be ter-
minalized with the exception of the link between the computer
terminal 60 and the security verification system 168, which
may be preserved to determine if a new user is attempting to
use the computer terminal 60 to log onto the computer net-
work 194. In this manner a physician’s access to the computer
network 194 is restricted while logged off and enlarged while
logged on.

[0172] This computer terminal access security operation is
described more particularly in steps 676 through 692 of FIGS.
15D-15E. The value of the idle/invalid link counter is com-
pared in step 676 to a predetermined disable I/O limit. If that
value does not exceed the disable I/O limit, the periodic
polling continues with step 656. If and when the value of the
idle/invalid link counter does exceed the disable I/O limit, in
step 684, the input and output devices of the computer ter-
minal 60 are disabled, if they have not been previously disabled
(step 680). In step 688, the value of the idle/invalid link
counter is compared to a predetermined logout limit. Periodic
polling is continued in step 656 if the value of the idle/invalid
link counter does not exceed the logout limit. If and when this
value is exceeded, in step 692 the physician is logged off
the computer terminal 60 and information stored in memory or
cache on the computer terminal by the user is overwritten.

[0173] If the content of the recommitment response signal is
valid (step 668), in step 696 the security verification system
168 processes the signal through a verification algorithm,
attempting to decrypt the signal with public keys and com-
paring the decrypted output with the original recommitment
signal. If the decrypted output matches the original recom-
mitment signal (step 700), then in step 704 the computer
network 194 recognizes that the physician is still using the
computer system. The idle/invalid link counter is reset and the
display and other input and output functions of the computer
terminal 60, if disabled, are restored. If the decrypted output
does not match the original recommitment signal (step 700),
then in step 708 the computer network 194 recognizes that
another physician is nearby. If the value of the idle/invalid
link counter exceeds a third limit (step 712), then the original
physician is logged off, memory cache and temporary work
space utilized by the original physician or applications
executed by or through the original physician is deleted and/
or overwritten, and the new physician is logged on to the
computer terminal. If the value of the idle/invalid link counter
III. OPERATION OF AN ICD IN ACCESS CONTROL

[0175] FIGS. 16A-16F describe the operation of an ICD 10 (FIG. 1) in responding to interrogation and recommitment signals transmitted by a proximately located computer terminal 60 (FIG. 3). In order to conserve power, the ICD 10 is preferably capable of alternating between sleep and wake states. During a sleep state, the ICD 10 is not responsive to signals transmitted by computer terminals 60 and other proximate smart devices, and may be essentially "invisible" to such devices. This alternating sleep/wake cycle is described in steps 724 through 732. In step 724, the ICD 10 maintains a wake state in which it is capable of receiving and transmitting signals through its wireless communication means 14. If in step 728, the time allotted for the wake state has expired and no signal has been received via the wireless communication means 14 of the ICD 10, then in step 732 the ICD 10 is powered down for the allotted duration of its sleep state, before cycling back to the wake state of step 724.

[0176] If a signal is received during its wake state, however, the alternating sleep and wake cycle is suspended in order to process and respond to the signal. In step 736, the ICD 10 processes and identifies the signal. If the signal is identified as a nonspecifically addressed signal (step 740) or as being addressed to the instant ICD 10 processing the signal (step 742), then further evaluation of the signal is performed, beginning with step 760, discussed infra.

[0177] A signal that is neither nonspecifically addressed (step 740) nor specifically addressed (step 742) to the instant ICD 10 is regarded as being extrinsically addressed to a second ICD 10. This situation may arise when two system users 68 with two security badges 10 are in the vicinity of the same computer terminal 60, one of them being logged onto the computer terminal 60. In step 744, the extrinsically addressed signal is evaluated to determine whether or not it is of a nature seeking an identification signal from the second ICD 10. If not, the instant ICD 10 ignores the extrinsically addressed signal and retires to wake state 724. If, however, the extrinsically addressed signal is of a nature requesting an identification signal, in step 752 the instant ICD 10 pauses to permit the second ICD 10 to transmit its identification signal. In step 756, the ICD 10 then transmits its own identification signal to the computer terminal 60 to indicate its presence, retiring afterward to wake state 724. This may allow the security verification system 168 to temporarily blank the screen to prevent unauthorized access to data by one physician through the access privileges of another physician. Alternatively, after repeated failures by the computer terminal 60 to receive a response signal from the second ICD 10, the second physician may be logged out and the instant physician logged in.

[0178] In the event that the signal was either nonspecifically addressed (step 740) or specifically addressed to the instant ICD 10 (step 742), the operation advances to step 760, where the signal is further evaluated to determine whether it is an interrogation or recommitment signal, in which case it would have been encrypted by a private key of the security verification system 168. If in step 760 it is identified as an interrogation or recommitment signal, then in step 764, a key ID tag appended to the signal is used to locate the public key stored in the memory element 262 (FIG. 6) of the ICD 10, with which it decrypts the signal.

[0179] In step 768, the decrypted signal is evaluated for information positively or probabilistically identifying the security verification system 168 as the source of the signal. This step implements the precaution of programming the ICD 10 to detect and reject interrogation signals that are too short or probabilistically non-random. If the decrypted signal is not distinguishable as originating from the security verification system 168, then in step 772, the ICD 10 stores and transmits an invalid message code, retiring to wake state 724. If the decrypted signal is recognized as originating from the security verification system 168 (step 768), then in step 774, the signal or a portion thereof is re-encrypted using the private key of the ICD 10 and transmitted, in step 776, to the computer terminal 60. Following this transmission, the ICD 10 retires to wake state 724.

[0180] Turning back to step 760, if the signal is not identified as an interrogation or recommitment signal, in step 784 the signal is evaluated to determine whether it is prompting the ICD 10 to transmit stored data to the computer terminal 60, in which case in step 788 the data is transmitted before the ICD 10 retires to wake state 724. If the signal was not identified as a prompt for data transfer (step 784), then in step 794 the signal is evaluated to determine whether it is prompting the ICD 10 to delete specified data, in which case in step 796 the specified data is deleted before the ICD 10 retires to wake state 724.

[0181] If the signal was not identified as a request to delete specified data (step 792), then in step 800, the signal is evaluated to determine whether it is prompting the ICD 10 to digitally sign a document or data record using its private key. If the signal is not identified as a request to digitally sign a document, the signal is treated as an unspecified command, upon which the ICD 10 takes no action, instead retiring to wake state 724. If the signal is identified as requesting a digital signature (step 800), in step 804 the computer terminal 60 or the ICD 10, by means of its audible alerting device 20, prompts the physician to depress the activation button 18. In step 808 the ICD 10 waits for the physician to respond for a limited time period. In step 812, if the activation button 18 has not been depressed before the expiration of this limited time period, then in step 816 the ICD 10 returns a signal indicating that the signature has not been provided, retiring then to wake state 724. In this manner a digital signature will not be provided without the affirmative agreement and action of the physician. If in step 812, the activation button 18 had been depressed within the limited time period, in step 820 the document, a message digest or an information packet is encrypted in whole or in part and transmitted to the computer terminal 60, the ICD 10 afterward retiring to wake state 724.

[0182] Though not illustrated, the activation button 18 may be pressed for several seconds in order to suspend automatic log on access to a computer terminal 60 without being
prompted to enter a password. The ICD 10 may emit an audible sound to indicate that automatic log on has been suspended.

In addition, while the preferred embodiment is described above wherein a terminal initiates an interrogation process, it is also possible in other embodiments to initiate an interrogation via the ICD either every time an ICD is proximate a terminal or when an earmarked ICD button is pressed.

**IV. BROWSER INITIATION**

It is contemplated that the inventive ICD/smart device system will be used with conventional computer terminal hardware which can be employed to run other useful software programs. To this end, when a physician nears a terminal and the terminal and the physician’s ICD 10 perform an interrogation, the physician will simply be logged onto the terminal and ICD information packets may or may not be automatically transferred to the terminal, depending on how the terminal is configured. In a preferred embodiment, after a successful interrogation, a terminal automatically queries an ICD 10 to retrieve information packets for display. In another embodiment, after a successful interrogation, a physician is given the option to use any terminal capabilities which the physician is authorized to use. For example, in addition to downloading information from the physician’s ICD to the terminal, the physician may wish to use a word processor or a spreadsheet, access the Internet, access e-mail and so on. In this embodiment, upon accessing a terminal, the physician is given the option to select any of several different applications. Instead of automatically querying an ICD 10 for information packets to transmit packets, a physician must press activation button 18 (see FIG. 1) at which point packets are transmitted.

In either of the above embodiments (i.e. automatic and manual packet transfer), when not using a terminal to display packet information, the terminal must be useable for other applications.

To enable a terminal to facilitate various applications and still be ready to receive ICD 10 data, preferably, a split screen is maintained by the terminal. Referring to FIG. 22, an exemplary split screen 523 is illustrated. Screen 523 includes an upper window 525 and a lower window 527. Although illustrated as relatively large, in reality, lower window 527 is extremely small (e.g. a single line) so that a selected application can take essentially full advantage of entire screen area 523. Generally, a selected application (e.g. a word processor) runs in window 525.

Exemplary HTML code for controlling window 525 is indicated in box 901. Lines 903 and 905 indicate that the information from www.ab.com and from address ls:swap.htm, respectively, should be displayed in windows 525 and 527, respectively, wherein “I” corresponds to the address location associated with the input device and acts as a device similar to a disk drive. In window 527 code segment 529 is provided at a time 1 prior to information being provided at address ls:swap.htm, Segment 529 includes a “Refresh” command 907 and a command “url=ls:swap.htm”. Refresh command 907 indicates that window 527 should be refreshed periodically (e.g. every 3 seconds) with data stored at address ls:swap.htm. Where no data is stored at address ls:swap.htm, window 527 remains relatively small (e.g. a single line at the bottom of the screen). However, upon a refresh cycle, when information has been provided at ls:swap.htm, window 527 is automatically expanded such that the information can be displayed therein.

When an information packet is received from an ICD 10, either through automatic query or pressing button 18, the packet is stored at ls:swap.htm which emulates a disk drive and segment 529 is the code sample in the file.

Thus, after an ICD 10 first establishes communication with a terminal, until information packet transmission to the terminal, a physician can use any of several different terminal applications in window 525. However, once an information packet is received, code line 909 expand and refresh window 527 with a screen which is configured via the received information packets.

For example, assume a physician’s ICD 10 includes three patient information packets which the physician is to review via a terminal. Prior to receiving the packets, however, the physician would like to review data on ABC Corporation which is accessible via the Internet. When the physician is proximate a terminal, the terminal and ICD 10 perform an interrogation process and, after a successful interrogation, the terminal allows the physician to access the terminal. In the first embodiment (i.e. automatic packet query), the input device automatically retrieves the ten packets from the ICD 10 and stores the packets on disk address 1. The next time (e.g. within 3 seconds) screen 523 is refreshed, the browser displays a screen configured accordingly to the packets stored at address ls:swap.htm.

Referring to FIG. 24, an exemplary HTML code segment 911 which may be provided at a time 2 to address ls:swap.htm via an ICD 10 and a resulting terminal screen 499 are illustrated. Segment 911 expands window 527 and reduces window 525 and provides three different types of information including a summary phrase 501, separate record or information unit summaries in a table 913 and interaction icons 503 and 505. Phrase 501 summarizes table 913 information and in the example indicates there are three records to review. Table 499 presents the records to review in summary form. The interaction icons include REVIEW and STORE icons 503, 505, respectively.

Either of icons 503 or 505 may be selected using a mouse controlled cursor (not illustrated). Because the physician wishes to first use the Internet to access ABC Corporation data, the physician selects STORE icon 505 whereupon the physician selects STORE icon 505 which stores the packets on a terminal or network memory device for later review. Thereafter, screen 523 (see FIG. 22) is redisplayed, including expanded window 525 and reduced window 527 (see FIG. 22). Window 527 waits for additional packets on drive 1. In window 525 a personal menu of icons representing applications for the accessing physician is provided, one of the selectable icons corresponding to the physician’s Internet account. The physician selects the Internet icon, reviews ABC Corporation data and can then return to an application which allows review of the stored packets.

Referring to FIGS. 1 and 22, in the second embodiment where packets are not transmitted until button 10 is pressed, when a physician gains access to a terminal, screen 523 is initially displayed, the physician’s personal menu of application icons displayed in window 525. In this case, the physician selects the Internet icon, reviews the ABC Corporation information and then closes the Internet application.

At any time while the physician maintains access to the terminal, the physician may press button 18 to transmit information packets to the terminal. When button 18 is pressed, packets are sequentially stored to and at ls:swap.htm and then provided to the terminal. Upon the next refresh cycle...
(e.g., 3 seconds), an initial screen (see FIG. 23) characterizing the packets and providing options is provided.

V. INTERROGATING ICD

[0195] Referring now to FIGS. 1 and 23, a preferred embodiment of the ICD badge 10 is identified as ICD 401. ICD 401 is essentially identical to ICD 10 (FIG. 1) having the same internal components, an alarm indicator, a speaker, an audio digitizer, a transceiver, a visual indicator (e.g., picture, text, etc.) and so on. However, ICD 401 is different than ICD 10 in that the activation mechanism is different.

[0196] FIG. 23 is a perspective view of ICD 401 showing, generally, the back side of ICD 401, the front side of ICD 401 appearing as illustrated in FIG. 1. Instead of having a conventional activation button (26 in FIG. 1), ICD 401 includes an interrogating activation button 403 which includes a fingerprint pad 405 which is approximately the size of a thumb. Pad 405 is capable of discerning the characteristics of a fingerprint when a thumb is pressed thereon. Various systems for discerning fingerprint characteristics have been provided in the prior art and therefore will not be explained here in detail. Suffice it to say that any method for discerning characteristics may be used here which can be implemented in a relatively small electronic package. Pad 405 is linked to the ICD processor (see FIG. 6) and provides print characteristics to the processor for interrogation.

[0197] Because each ICD 401 is an identification badge, each ICD 401 is uniquely associated with a single physician. Therefore, when an ICD 401 is initially provided to the physician, the physician commissions the ICD 401 by placing the physician's thumb on pad 405 a first time. During a commissioning protocol, the first time a thumb is placed on pad 405, the ICD processor discerns fingerprint characteristics and stores the discerned characteristics in an ICD memory (see FIG. 6). In addition to storing fingerprint characteristics, the ICD processor is equipped with code for comparing fingerprint characteristics and based on the comparison, for either allowing ICD functions to be performed or disabling ICD 401.

[0198] To this end, prior to ICD 401 being used for any information gathering, transmitting, generating or interrogating purposes, a physician must place her thumb on pad 405 pressing button 403. With her thumb on pad 405, the ICD processor again discerns fingerprint characteristics and compares the discerned characteristics with the stored characteristics. Where the discerned and stored characteristics are essentially identical, ICD 401 is enabled. Upon a match ICD 401 may either be programmed to be enabled for one transaction or a certain number (e.g., 10) of transactions or, in the alternative, may be enabled for a specific time period or, where ICD 401 is used to perform a transaction within a specific time window, may remain enabled for a subsequent period.

[0199] Where the discerned fingerprint characteristics do not match the stored characteristics, ICD 401 may do any of several different things. First, ICD 401 may simply disable itself until an authorized facility administrator resets the ICD 401 for another identification attempt. Second, ICD 401 may allow several (e.g., 3 or 4) attempts to generate a match and only after several failed attempts disable itself. Moreover, when ICD 401 disables itself, ICD 401 may either cause an audible or a visual signal indicating a mismatch and may continue to cause the signal to alert passersby that an unauthorized person attempted to use the ICD 401.

[0200] ICD 401 is uniquely advantageous for a number of reasons. First, ICD 401 ensures that only a specific physician associated with ICD 401 can use ICD 401 for collecting, generating, and transmitting information and for interrogating other smart devices. This is particularly important, as will become clear below, in instances where successful interrogation enables a physician to perform some procedure or to administer some drug. For example, one example explained in more detail below allows a physician to open a drug container (see FIG. 5) only after a successful interrogation is completed between the container and an ICD 401. The interrogation is meant to ensure that the user of ICD 401 is authorized to administer the drug inside the container. While the interrogation provides one level of security, there is no way to ensure that a physician's ICD 401 will not be misplaced or stolen in an attempt to misdirect a patient. With ICD 401, even if the ICD 401 is stolen, a would-be mismedicatior could not open a drug container unless the physicians fingerprint could also be duplicated.

[0201] Second, while other systems for identifying personnel via fingerprint or other biometric indicia are prevalent in the prior art, many such systems require that users "give up" control of their indicia by providing the indicia to a system administrator. For example, a security system for restricting access to an office building may include a security server and a plurality of fingerprint pads located at building entrances and perhaps at other doors located throughout the building. The security server has access to a memory storage device where fingerprint characteristics corresponding to each person who has authority to access the building are stored. To enter a building, a person places her thumb on a pad, the pad discerns fingerprint characteristics which are provided to the server and the server compares the characteristics to all sets of fingerprint characteristics which correspond to personnel who have authority to access the building through the specific door. Where discerned characteristics match a stored characteristic set, the building allows entry. If the discerned and stored characteristics do not match, the building restricts entry.

[0202] Unfortunately, with the system described above, each of the people whose fingerprint characteristics are to be examined during an access attempt must agree to provide their fingerprint characteristics to the security server to enable comparison. While providing such biometric indicia is not difficult, many people object to giving and only grudgingly give, such information as they feel that type of information is private. Clearly, if every building a person entered would have to have personal biometric indicia, peoples biometric information would be virtually everywhere.

[0203] Another problem with such a system is that, like a door handle, many (e.g., hundreds and even thousands) people may be placing their thumbs on a single fingerprint thumb pad every day. Such access to the pad not only seems unsanitary but in fact is unsanitary as germs are spread via the pad.

[0204] With the inventive ICD 401, all personal biometric indicia remains personal and does not have to be "given up" to some administrative server. This is because ICD 401 and not some amorphous server, performs the interrogation and enables ICD 401 to operate. Thus, personal biometric indicia is never accessible by a device outside a physician's own ICD which the physician controls to at all times.

[0205] In addition, with ICD 401 only the physician who "owns" ICD 401 will be placing her thumb on pad 405 unless some mistake is made. Thus, ICD 401 is relatively sanitary,
Another advantage of ICD 401 is that, because ICD 401 is only usable by a single physician, only a single set of fingerprint characteristics have to be stored by the ICD processor and discerned characteristics during an interrogation need only be compared to a single set of stored characteristics. These advantages cut down both on required memory and processor time necessary to complete an interrogation which means that ICD 401 need only a relatively simple processor.

It might also be noted that while the fingerprint pad activation button has been described in the context of ICD 401, clearly this aspect of the present invention could be used in many other technical areas. For example, in the case of a building entry security system as described above, a smart card may be provided which is similar to ICD 401 except that, upon enablement, the card may only be able to unlock a door. In this case, to open a locked door, first, a user places his thumb on a smart card fingerprint pad similar to pad 408 (see FIG. 23). The pad discerns print characteristics and provides those characteristics to a card processor. The processor compares the characteristics to a stored characteristic set corresponding to the card owner. Only if the stored and discerned characteristics are essentially identical will the card be enabled to unlock the door. When the card is enabled, rather than indicating the fingerprint characteristics to the security server, the card sends out an identification signal to a receiver (e.g. RF or infra-red) which provides the identification signal to the server. The server then compares the identification signal to stored valid identification signals to determine if the received signal corresponds to a person who is authorized to open the door. The door is only opened if a match occurs. In this manner a security system which uses personal biometric indicia can be provided without requiring users to give up control of their indicia.

Moreover, the fingerprint pad activation button could also be used in the context of a credit card to enable or disable a credit card on the basis of a simple fingerprint check as described above with respect to the access card. To this end, to charge a purchase, a user places a thumb on a pad, a comparison is performed and, only when a match occurs is a purchase authorized.

While the inventive pad activation button has been described above in the context of a fingerprint pad, the invention is not meant to be so limited and any other recognizable biometric indicia or uniquely personal biomedical indicia could be used to activate a properly configured activation button. For example, a retinal scanner, voice recognition identifier, skin texture identifier, etc., could be used to activate a button and so on.

VI. OPERATION OF AN ICD IN COLLECTING DATA

FIGS. 17A through 17C describe the operation of an ICD 10 in gathering and exchanging data with smart devices with which ICD 10 is in communicable range. This operation is described particularly, but not by way of limitation, in the context of a hospital, where the exchange of information between ICD 10 and a plurality of smart devices assigned to various patients and distributed throughout the hospital may be limited by the access privileges corresponding to patients whom or with whom a physician is authorized to diagnose, treat, or interact. Referring again to FIG. 4, a single hospital room 104 (FIG. 4) may include a number of smart devices, including a computer terminal or workstation 60, a patient identification display 100, a bedside communication device 96, a patient treatment device 116, and a patient monitor 80, each of which may communicate with the ICD 10 or, in some circumstances, with each other.

Generally, smart devices like bracelet 40 (see FIG. 2) or container 200 (see FIG. 5) include information about a patient or a medical event and/or generate information about a medical event, the included or generated information being stored on a device or more information segments in respective device memories. When a physician decides to collect information from a smart device, the physician establishes communication between the device and the physician's ICD 10 and causes the smart device to transmit stored information segments to ICD 10. For the purpose of this explanation, the term “data record” is used to describe a grouping of information which is to be transferred among system devices and may include a simple information segment or a more complex construct such as an information packet referenced above and described in more detail below.

When ICD 10 receives one or more information segments, ICD 10 recognizes the nature of the segments and stores related segments as an information unit in HTML format. In addition, ICD 10 may also generate other information segments which can be added to received segments to provide enhanced information units. Exemplary additional segments may include a time and date stamp generated by badge processor 250 (see FIG. 6) and physician identifying information (where available).

Moreover, ICD 10 also provides two other types of information. First, ICD 10 includes an address specifier (i.e. the ICD processor) which provides a server target address for each information unit formed. The target address specifies a specific server or database address to which the information unit should be sent for storage or processing on system 194 (see FIG. 7). Second, ICD 10 also provides browser formatting information which indicates how browser 115 should present information in an associated information unit on display 103.

For each information unit browser 110 assembles an information packet which includes the information segments in each unit, an associated server address and relevant configuration information. Importantly, each information packet assembled by an ICD 10 is in HTML format so that the packet can be received by a conventional browser 115 for display.

Subsequently, after a physician has gained access to a terminal 60 (see FIG. 3), the physician causes information packets assembled by the physician's ICD 10 to be transmitted to the terminal 60 via an input device 64. The packets are received and read by browser 115. Browser 115 displays information unit information in the format indicated by the configuration information and stores the relevant server target address.

In addition to indicating how information unit information is to be configured on display 103, configuration information may also provide on-screen tools for modifying some or all of the unit information displayed. For example, where displayed information specifies a medication dose which was supposedly delivered to a patient, while the displayed dose may indicate the dose dispensed by a pharmacy, upon administration, a physician may have elected to modify the dose. In cases where such modifications can be anticipated, the configuration information provides a tool (e.g. a pull down window) for modifying the displayed dose prior to storing the unit information.
Moreover, the configuration information may also facilitate hyperlinks to additional information which is related to displayed information. For example, again, in the case where a medication is dispensed, displayed information will typically include the dispensing physician’s name. In this case, the configuration information highlights the physician’s name and provides a hyperlink address “behind” the physician’s name to a biography site specifying information about the physician. Similarly, a patient’s name or identification number may be linked to a medical history record for the patient via hyperlink.

After a physician reviews and perhaps modifies displayed information packet information, the physician approves the information by selecting an approval icon on display. When icon is selected, browser causes an “electronic signature” to be attached to the approved information in a manner described in more detail below. Thereafter, browser sends the approved information to the server target address for storage and/or processing.

In the preferred embodiment, data exchange between an IC 10 and a smart device associated with a particular patient is conditioned upon, and must be preceded by, establishing an “association” between a physician using an IC 10 and the patient with whom a smart device is associated. Preferably, an association is digitally recorded by the IC 10 in the form of information uniquely identifying the patient, the smart device and/or the IC 10 itself, and the time and date of the association. This information may later be appended to information packets exchanged with smart devices and computer terminals, providing information packets with a complete audit trail. Further, smart devices and IC 10s themselves may also digitally record associations in a similar fashion.

Referring to FIGS. 1 and 1A, at step 824, a physician attempts to initiate a communication link or exchange information with a smart device by pressing the physician’s IC 10 proximate a smart device and pressing IC 10 activation button (FIG. 1). Depending on the sophistication of IC 10 and the smart device and the sensitivity of the information to be exchanged, the communication established with the smart device may or may not utilize public key cryptography. While link initialization may be automated rather than user-initiated, making the links user-initiated allows IC 10 to conserve energy and prevents unnecessary link initialization with devices with which a physician is not concerned. Alternatively, the smart devices may be individually and manually enabled to communicate through the use of activation switches incorporated in the smart devices. Provided that the signal path between an IC 10 and a smart device is substantially unobstructed and short enough that signal transmissions are not excessively attenuated, a communications link is established.

In step 828, IC 10 evaluates the existence, if any, of an association between the IC 10 and any patient (not necessarily the particular patient to which the linked smart device is directed). An association exists if IC 10 has most recently been used with a smart device which is associated with a patient. In this case, IC 10 stores information specifying a specific patient. For the purposes of this explanation it will be assumed that the identifying information comprises a patient’s identification number which, if an association exists, is stored as an identification information segment by IC 10. Thus, to determine if an association exists, IC 10 determines if an identification information segment is occupied. If there is no association, in step 832 IC 10 transmits to the smart device its own identification information and a request for information to be returned. If there is an association, in step 836 IC 10 transmits its own identification information, patient identification information (of the patient with whom IC 10 is associated), and a request for data to be returned.

Steps 832 and 836 are each followed by step 840, in which IC 10 waits for a predetermined time period for a response from the linked smart device. If no response is received within the predetermined time period (step 848), then in step 852 IC 10 emits a first audible sound to alert the physician that no response was received from the smart device. In step 856 the operation initiated by the physician in step 824 is terminated. If instead a smart device transmits a response in the form of a recognizable information segment which is received before the predetermined time period elapses (step 848), then referring also to FIG. 17B, in step 860 the data record or information segment contained in the response signal is stored. In addition, referring also to FIG. 6, processor 250 identifies the time and date via clock 254 at which the information was received and stores a time stamp as a second information segment, combined with the received information segment, as an information unit.

One type of information segment or data record which may be transmitted to an IC 10 is a patient identification record. An exemplary record is illustrated in FIG. 9 and includes an identification number, name and distinguishing characteristics. All or only a small part of the information illustrated may be included in a transmitted record but at least the identification number is transmitted.

If the data record or information segment stored in step 860 is a patient identification record (step 864), and if IC 10 is already associated with the patient indicated by the record (step 868), then in step 876 IC 10 emits a second audible sound readily distinguishable to the human ear from the first audible sound of step 852, signaling to the physician that IC 10 is associated with the patient and that the exchange of information was successful.

If the data record or information segment recorded in step 860 is a patient identification record (step 864), but IC 10 is not associated with any patient (steps 868 and 872), then in step 874 IC 10 records the patient’s identification number in the identification information segment to establish an association and in step 876 emits said second audible sound.

If the information segment recorded in step 860 is a patient identification record (step 864) identifying a first patient, but IC 10 is associated with a second patient (steps 868 and 872), then in step 878 the association with said second patient is closed and a new association is established by recording the first patient’s identification number in the identification information segment. In step 880 IC 10 emits said second audible sound twice to indicate the closure of a previous association and the initiation of the current association.

If the data record information segment recorded in step 860 is not a patient identification record (step 864) but if IC 10 is already associated with a patient (step 888), then in step 892 the data record is modified. In this regard, the received information segment is combined with the current identification information segment (i.e. the segment which identifies the patient with which IC 10 is currently associated) and perhaps other information segments to form an information unit (i.e. an enhanced data record). The other
information segments may include a time stamp segment, a physician segment and so on. The information segment received and other information segments which identify both the physician and the patient (i.e. the identifying information previously recorded in establishing the current association between ICD 10 and patient) are combined to form an information unit. Further, the ICD 10 emits said second audible sound to indicate the successful transaction.

[0228] If the data record or information segment recorded in step 886 is not a patient identification record (step 864) then if ICD 10 is not currently associated with a patient (step 888), then in step 896 the data record is modified to include identification information attributable to the physician to which ICD 10 is assigned. To this end, the received information segment is combined with a physician information segment which identifies the physician and perhaps other information segments (e.g. a time stamp) to form an information unit. Further, the ICD 10 emits said second audible sound to indicate the successful transaction.

[0229] Although not illustrated by flow chart, association of ICD 10 with a patient may be manually terminated by depressing activation button 18 for a few seconds, after which ICD 10 emits an audible sound to indicate that the association has been terminated. An association with a patient may also be automatically terminated after a sufficient period of inactivity with respect to ICD 10.

[0230] FIG. 14A illustrates an exemplary HTML coded information packet 440 which corresponds to a medication dispensation event and which is provided by an ICD 10. Packet 440 may be provided in any of several different ways.

[0231] First, packet 440 may be constructed by ICD 10 as ICD 10 receives certain types of information. In this case, ICD 10 is provided with packet configuring software which recognizes information segment type and thereafter tailors a specific packet for the received segment.

[0232] Second, packet 440 may be constructed primarily by some other network device and provided to ICD 10. For example, referring again to FIG. 7, dose dispenser 150 dispenses medication for administration. The type of information generated during administration is often very similar (e.g. time, date, type, dose, patient ID, physician ID, etc.). In this case, dispenser 150 may provide a general packet format to a medication container (see FIG. 5) which is in turn provided to ICD 10 when a drug is administered.

[0233] Third, a smart device (e.g. an IV pump) may provide a general packet format including target address along with data provided to an ICD 10.

[0234] In FIG. 14A, packet 440 includes a target address field 444 which specifies a server address to which packet information is to ultimately be delivered. The exemplary target address includes a hospital name, an event type (“medication”) an event specifier (“given”), a patient identification number (“987654321”), an event date and an event time. Packet 440 also includes a report type indicator 448, a field 452 for indicating that patient ID has been verified and format medication quantity fields and 456 and 460 indicating how much of the dispensed medicines was administered. To this end, fields 456 and 460 are set up so that, initially, each format field 456, 460 causes the medicine dose dispensed to be displayed. In addition, fields 456 and 460 provide interaction tools for modifying the displayed dose to reflect actual administered doses. Thus, field 456, which corresponds to Penicillin dose, allows a physician to modify an initially displayed dose of 2 capsules by selecting either 1.5, 1, 0.5 or none as the actual administered dose. Similarly, field 460, which corresponds to Tylenol dose, allows choices of 1, 0.5 and none to identify administered dose.

[0235] Packet 440 also includes a physician identification field 464, and a data and time field 468 indicating time of medication administration. Packet 440 further includes a dispense identification field 468 indicating the physician who dispensed the specific medication, the date and time of the dispensation and so on. Hidden fields 472 which incorporate information to be transmitted along with information to be displayed but concealed from view through the browser display, may also be added. Information appropriately concealed may include initial quantities of medication dispensed, which information may be compared with the amount actually administered. Packet 440 further includes an approve field 476 which specifies configuration of an APPROVAL icon on display 103. The APPROVAL icon allows a physician to approve of information displayed via browser 115. When field 476 is displayed and an associated icon is selected via browser 115, information in packet 440 is transmitted for storage to a database 158 or 162 at the server target address indicated in field 444.

[0236] Referring also to FIG. 14B, an exemplary browser screen 480 which corresponds to packet 440 is illustrated. Screen 480 includes a plurality of elements which indicate all information associated with a drug administration event. The elements, which correspond to identically marked fields in packet 440 (see FIG. 14A), include an identification element 445, a report type element 448, an ID verification element 452, a medical dose element 456 and 460, an administrating physician identification element 464 including date/time 469, a dispensing physician identification element 468, and approval icon 476. When formatted data packet 440 is transmitted to a terminal 60, the ICD 10 may be programmed to emulate a file structure device, wherein the open file command of the browser 480 may be used to request data from the ICD 10.

[0237] Thus, generally, ICD 10 formats an information packet (i.e., in the present example, a medication administration record) for delivery to network system 194 via a computer work station 60 which includes three types of information. The three information types include general information (including, perhaps identification information) to be stored, a target server address (i.e. a target address field) at which the general information is to be stored and browser screen configuration information (i.e. format fields) indicating how the general information to be stored should be displayed for review, modification and approval by a physician.

[0238] In addition to receiving information from a smart device, ICD 10 is also capable of receiving dictation for storage in one or more information units for delivery to system 194. Referring to FIGS. 1 and 18, while observing or treating a patient, a physician may, in step 900, press dictation button 26 and dictate messages (step 904) into microphone 22 of ICD 10. Digitizing circuitry incorporated in processing circuitry 260 (FIG. 6) digitizes the message (step 904), which is recorded as a message record or dictation information segment in memory element 262. If ICD 10 is associated with a patient at the time the dictation is recorded (step 908), then in step 912 patient identification information and a time stamp are incorporated into the message record. To this end, ICD 10 combines the identification information segment, the time segment and the dictation information segment into an information unit. Further, in step 912 a database address or
server target address is formulated for the information unit using the time stamp, the dictation data type and patient identification information. Further, in step 912 the ICD 10 emits said audible sound. If the ICD 10 is not associated with a patient at the time the dictation is recorded (step 908), then in step 916 a time stamp segment is added to the dictation information segment to form an information unit. Further, in step 916 the ICD 10 emits said audible sound.

[0239] Dictation information is treated like any other gathered information in the sense that ICD 10 formulates an information packet including a segment associated with the collected information. The only difference is that the collected information is digital audio. It is contemplated that when a packet includes a dictation segment, ICD 10 will construct a packet including a field which will provide a “Dictation” icon associated with the dictation segment, the icon being displayed when the packet information is reviewed via browser 115. When the dictation icon is selected, the dictation associated therewith is replayed via terminal 60 for physician review. In addition, other icons for controlling dictation review (i.e. fast forward, reverse, stop, pause, etc.) may be configured via packet configuration information.

[0240] In addition, it is contemplated that in many instances both statistical information and audio dictation may be collected during a single patient visit. In this case, ICD 10 may do one of two things. First, ICD 10 may formulate a single message packet which includes all collected information and appropriate browser configuration information. In addition, in this case, if appropriate, ICD 10 may be programmed to generate more than a single target address for all of the packet information or, different target addresses for the various types of packet information. For example, while a dictation segment should be transmitted to a transcription server for conversion to text (either manually or automatically by voice recognition software), medication administration information should be provided to the pharmacy server for logging and to determine if proper administration occurred. Either all information could be provided to both the transcription and pharmacy servers or only relevant information may be provided to the respective servers.

[0241] Second, where more than a single type of information is collected during a single patient visit, ICD 10 could be programmed to formulate two separate information packets for delivery to a terminal 60, a separate packet corresponding to each information type. For instance, in the example above, one packet may be formulated for dictation while a second packet is formulated for statistical information. While various packet schemes are possible, the preferred scheme provides only a single information packet for each patient visit which would include all types of information collected. This scheme has the advantage of maintaining a complete record for each patient visit which can be stored in a patient’s historical records to memorialize all aspects of this visit. Then, if specific servers require specific collected information (e.g. dictation, administration, administering physician, etc.), a central server can determine which information should be sent to each specific server.

[0242] In addition to generating specific information packets for transmission to browser 115, ICD 10 is preferably programmed to construct an initial screen packet. The initial screen packet, like other information packets is formatted in a conventional language such as HTML so that, when received by browser 115, browser 115 can display packet information as specified. The initial screen packet will typically include information which summarizes other packets to be transmitted to a terminal 60 and configuration information. For example, where ten information packets are to be transmitted to a terminal 60, the summary information may simply indicate, “There are 10 patient records to review.” The configuration information indicates how the summary information should be displayed, may provide instructions and typically provides icons for physician interaction. Exemplary icons include a “REVIEW” icon and a “STORE” icon. An exemplary initial screen 499 is illustrated in FIG. 24 and includes a prompt phase 501 and icons 503 and 505.

[0243] Referring to FIG. 3 when ICD information packets are transmitted to a terminal 60, the initial screen packet is also transmitted. The input device 64 receives all packets, distinguishes the initial screen packet from other packets, stores the other packets in RAM 109 and provides the initial screen packet to browser 115 for display. Browser 115 displays an initial screen (see FIG. 24) corresponding to the initial screen packet providing interaction icons REVIEW 503 and STORE 505.

[0244] If REVIEW icon 503 is selected, browser 115 accesses the first packet in RAM 115 and displays associated information as configured by the packet. After review of the first packet browser 115 displays record packet information and so on. If STORE icon 505 is selected, browser 115 stores the initial screen packet along with associated other information packets in RAM 109 (or some other suitable storage location) for later review and approval.

[0245] Other aspects, not included in FIGS. 17A through 17C, may be involved in communicating with or between certain smart devices. In one embodiment, the presence of a physician in proximity to a patient enables communication between the patient’s wrist bracelet 40 (FIG. 2) and the physician’s ICD 10. The communication link may be initiated by pressing the activation button 18 on the ICD 10 and/or an activation button (not illustrated) on the wrist bracelet 40, provided there is a complete signal path between the ICD 10 and the wrist bracelet 40. Once a communication link is established, ICD 10 identifies the patient and records the establishment of an association with that patient. ICD 10 may also request and receive additional information stored by the wrist bracelet 40, providing a beep, vibration or other sensation signal to indicate a successful transmission or to alert a physician. The wrist bracelet 40 may also record in its own memory the staff identification information and current date and time from the ICD 10 to provide an audit trail of the physicians who have associated themselves with the patient. If communication and association is established with another wrist bracelet 40 or, if not, after a preset period of time has elapsed, the ICD 10 regards the association to have terminated and alerts the physician to this fact with another beep, vibration or other sensational means of communication.

[0246] In another embodiment, the wireless communication means 52 of wrist bracelet 40 (FIG. 2) may utilize alternate communication means, such as magnetic coupling or low power radio transmission, rather than the preferred infrared means of the ICD 10. Similarly, the bedside communication device 96 (FIG. 4) of a patient bed 88 may also utilize alternate communication means. Further, the communication range of wrist bracelets 40 or other smart devices may be limited in order to prevent two devices from receiving the
same request. Instead of communicating directly with the ICD 10, the wrist bracelet 40 may communicate with patient identification display 100 directly or indirectly via communication with the communication means of a bedside communication device 96. A patient identification display 100 may also have transceiver device 64 compatible with the communication means 14 of the ICD 10. The smart devices may be arranged and implemented so that the patient identification display retrieves the patient identification information from the wrist bracelet 40 and electronically displays it. The patient identification display 100 may be programmed to cease displaying the patient identification information if the patient bedside device 96 no longer senses the presence of the patient. Patient chairs may be similarly equipped with smart devices to sense the presence of a patient and to convey such information to a patient identification display 100. Further, in order to establish an association with a patient, the ICD 10 may be required to establish a communication link with the patient identification display 100 instead of or in addition to the wrist bracelet 40, which patient identification display 100 would in turn transmit the patient identification information to the ICD 10. This would permit the transfer of patient identification information without the possible necessity of disrupting the patient in order to establish a communication link with the patient’s wrist bracelet 40.

[0247] If a new patient comes to occupy the patient room 104 or the patient bed 80, the patient identification display 100 obtains the new patient identification information from the wrist bracelet 40 worn by the patient and may be structured to transmit that information to the Admit, Discharge and Transfer System 166 (FIG. 7) of the computer network 194. Alternatively, the patient identification display 100 could display a request for input indicating whether or not the new patient is to be marked as having been transferred to the instant patient room 104. A patient monitoring device 80 (FIG. 4) or bedside treatment device 178 (FIG. 7) may reject a data exchange request from an ICD 10 if the physician wearing the ICD 10 is not authorized or cleared to diagnose or administer treatment to the patient. FIG. 12 illustrates the contents of the monitoring or treatment device information 380 that the bedside treatment device or patient monitoring device 80 may transmit to the ICD 10 if the data exchange is authorized. As part of a double-audit function, the monitoring device 80 or the bedside treatment device 178 would itself record any data transaction made with an ICD 10.

VII. ELECTRONIC SIGNATURE

[0248] Hereinafter, while information units and information packets as described above are still contemplated, other types of information such as word processor documents, spread sheets and the like are also contemplated and all such information types will be collectively referred to as documents.

[0249] An extremely important aspect of the present invention is that a physician’s identity is added to collected information or documents prior to long term storage or transmission to a server for further processing. By adding a physician’s identity, the system creates proverbial “ownership” of the document (i.e. information collected).

[0250] Taking this “ownership” one step further, according to another aspect of the invention, the information approval process which must be performed prior to long term document storage or transmission to a server requires a physician to take “responsibility” for approved documents. To this end, the present invention contemplates a digital signature procedure whereby, when a physician approves a document, the physician’s identity and, also preferably, an indication of the content of the document approved, are added to the approved document. This type of approval system helps ensure that documents are accurate. This is because, if a physician knows approved documents are to be recorded and attributed to the approving physician, the physician will be more careful to ensure document accuracy.

[0251] In one embodiment a simple text phrase is provided in a document approval field. For example, upon approving the phrase, “Dr. Smith approved this document on Tuesday, Aug. 25, 1998 at 10:30 AM”, may be added to the document.

[0252] The physician’s identity may be determined in any of several different manners. For example, as a physician’s ICD 10 must gain access to a terminal to review document information, the physician’s ICD 10 may, during the interrogation process, provide an indicator of the physician’s identification. In the alternative, each time an approval icon is selected the terminal may send a message to the physician’s ICD 10 requiring a physician’s digital signature. When the message is received the ICD 10 transmits the physician’s digital signature in encrypted form. In this case, when a terminal receives the encrypted digital signature the terminal deciphers the encryption and correlates a physician with the digital signature.

[0253] In another embodiment, when a physician logs onto a terminal in a conventional manner (e.g. entering a password via a keyboard), the terminal may identify the physician and subsequently add the physician’s identity to each document approved by the physician.

[0254] While a simple text phrase indicating approval suffices to convey that a specific individual approved a document at a specific time, such text phrases are relatively impersonal and therefore have relatively little value in terms of creating a “feeling” of responsibility for approved documents. Therefore, preferably, instead of providing an impersonal text phrase to indicate approval, a picture of a physician’s actual scripted signature (i.e. a signature picture) may be digitized and stored in an ICD memory, the signature picture provided to the terminal for insertion in the approval field along with the time and date of approval. The signature has traditionally been an indicator of responsibility and therefore indicates the import of the approval process to the approving physicians.

[0255] Unfortunately, even where a digital signature picture is provided, it is possible for an unscrupulous physician or some other unscrupulous person who has access to a stored document to effectively electronically modify the approval field by, for example, copying a physician’s digital signature picture from one approval field into another. While such copying may be accomplished electronically by cutting a signature picture from one digital document to another, such copying or forgery may also be accomplished after a digital document has been printed out in paper document form. For example, after a digital document is printed, a physician’s signature may be clipped out of a first document, taped on a second document and copied via a high quality copier thereby rendering a document which was seemingly signed by the physician.

[0256] To ensure authentic signatures on documents, the present invention further includes an electronic “watermarking” procedure. A watermark is a mark which is difficult to reproduce and which is “laid over” some other information generally for the purpose of identification and indicating
authenticity of the underlying information. For example, often a watermark will be provided on paper currency, the mark appearing like a water stain across a portion of the paper, hence the term “watermark”. Watermarks have also been used to mark copyrighted material, the marks subsequently used to identify any copies of the copyrighted material.

Unlike currency watermarks, electronic watermarks and differences there between often are difficult to perceive via the human eye. Instead, electronic marks include pixels within a displayed picture which have specific and known characteristics. For example, one electronic mark on a screen display may include modified white pixels where every 10th white pixel which appears within the picture is slightly grey. While the specific color is slightly different than other white pixels, the difference is not detectible by the human eye. Instead, a computer is required to identify the pixilated watermark. In this case, if an electronically marked screen is electronically copied, suitable software running on a computer can be used to analyze the copy and detect the electronic watermark (e.g. the unique pixel intensities). In addition, where an electronically marked document is printed out, the watermark should be reproduced as a printed mark which can be used for subsequent authentication. Moreover, where a printed document including a mark is copied using a high quality copier the mark should be reproducible and therefor useable to authenticate.

In addition to unique pixel shading, electronic marks can be provided by providing different pixel intensities, pixel intensity or shading designs, a uniquely configured pixel bar adjacent a graphic design and so on.

Like a digital picture, a physician’s digital signature picture includes perhaps thousands of pixels. Unique signature picture pixel characteristics can be provided which can be used to identify authentic signature pictures. Unfortunately, as with a screen, a copied signature picture will often include the watermark pixels and therefore an authentic signature picture, as opposed to an electronically or manually (i.e. physical cut and tape) copied signature picture, may be difficult to identify.

To overcome the problem of accurately copied watermarked digital signature pictures, the present invention includes a content varying watermark which is generated as a function of the content of a document to which a signature is applied.

Generally, according to the present invention, in addition to storing a physician’s signature picture, an ICD memory also stores a standard watermark (SM) which corresponds to the physician and a program for modifying the standard watermark SM as a function of document content (DC). When a document is to be electronically signed, the document is transmitted to the physician’s ICD 10. The ICD 10 recognizes the requirement for signature, retrieves the standard mark, marking program and signature picture, isolates document content, modifies the standard mark as a function of the document content, places the modified mark on the scripted signature picture or on the document itself, places the marked signature picture on the document in an approval field and retransmits the “signed” document to the terminal. The modified mark MM can be expressed as:

\[MM = f'(SM, f(DC))\]

wherein \(f\) indicates a function. Other equations for identifying the modified mark MM may be used. For example, mark MM may be a function of both the standard mark SM and document content DC (i.e. MM = f(SM, f(DC))) or may be a function of both standard mark SM and a different function of document content DC (i.e. MM = f'(SM, f(DC))), etc. An example of how this aspect of the invention operates is instructive.

In this example, it will be assumed that a physician is currently logged onto a terminal, has download various documents to the terminal for review and now wishes to approve a document prior to long term storage.

Referring specifically to FIG. 25, when a physician selects an approve icon to approve a previously reviewed document, at block 604 the terminal determines if a watermarked signature is required for the document to indicate approval. Where a watermarked signature is required, at block 603 the terminal transmits the content of the document to be “signed” to the physician’s ICD 10 along with a simple instruction indicating that a digital signature is required.

Referring also to FIG. 26, when the ICD 10 receives the document and instruction at block 650, ICD 10 recognizes the instruction and ICD control passes to block 652. In some cases a document may include minimal information and therefore it might be difficult to generate a distinct and difficult to decipher watermark MM. Therefore, although not a requirement of the invention, it is contemplated that, in one preferred embodiment, there will be a minimum or threshold document content (TDC) requirement which indicates the minimum amount of content required to generate a mark MM. Where the document content DC is less than the requirement TDC, additional information, either random or meaningful, is added to content DC prior to modifying the standard mark. Meaningful data may include the current time or date.

The additional information is not necessary to understand the meaning of the document. Therefore, it is contemplated that the additional data would typically be added to the document in some non-visual manner. For example, the additional data may be added as some hidden text in a hidden note field or the like. On the other hand, the additional data may be added as a visual bar having varying pixel intensities. The important aspect of the additional data is that the additional data enables a secure content specific watermark to be generated which is not easily subjected to decryption.

Referring again to FIG. 26, at block 652, ICD 10 compares the document content DC with the threshold requirement TDC. The comparison may be as simple as comparing the number of words or characters in the DC to a corresponding threshold number TDC. Where the DC exceeds the TDC, control passes to block 656. Where DC is less than the threshold requirement TDC control passes to block 654.

At block 654 ICD 10 adds additional text or numbers to the DC thereby generating a new document content. As indicated above, the additional data is preferably, although not necessarily, added so that it will not appear on the document when the document is displayed.

At block 656 ICD 10 retrieves the ICD user’s scripted digital signature picture and applies the signature picture to an appropriate and designated location (i.e. the approval field) on the document. At block 656 ICD 10 retrieves the standard graphic mark from the ICD memory and modifies the standard mark SM as a function of the document content DC (e.g. the original document plus any additional data added plus the digital signature picture) to generate a modified mark MM. At block 659 ICD 10 applies the modified mark MM to the scripted digital signature picture generating a watermarked signature picture.
At block 660 ICD 10 replaces the digital signature picture on the document with the watermarked signature picture and at block 662 ICD 10 transmits the “signed” document back to the terminal.

Referring again to FIG. 25, after having transmitted a document to an ICD at block 603 the terminal awaits return of a signed document at block 605. When a document is received by the terminal control passes to block 607. At block 607 the terminal determines if the received document was signed. At block 609, where the document has not been signed for some reason, the terminal indicates failure to sign. At block 611, where the document has been signed the terminal stores the signed document. In addition, to facilitate the “feeling” of ownership and responsibility for the signed document, the terminal may display the document with the physician’s scripted digital signature picture thereon.

To allow a physician to confirm that approval occurred it is contemplated that, according to at least one embodiment of the invention, after a terminal displays a document including a signature picture, and prior to storing the document to long term storage or transmitting the document to a server for further processing, the terminal may provide a “STORE” icon which, when selected, stores or transmits the document including the signature picture. When the STORE icon is selected the document is transmitted.

When an approved document is accessed at a subsequent time, if there is any doubt that a signature picture is authentic, the physician’s ICD 10 which was supposedly used to generate the signature picture can be used during an authentication process to re-generate the suspect document. Then, the suspect and regenerated documents can be compared to determine if the suspect document is authentic. Where the documents are dissimilar, an electronic forgery has been identified and the suspect document is identified as a forgery.

To confirm authentic approval, it is contemplated that, software which allows a physician to retrieve and review stored information will provide some authentication functions while each physician’s ICD will facilitate other required functions. For instance, in one exemplary embodiment the retrieval/review terminal software is capable of scanning in a watermarked signature picture from a hardcopy of a document, scanning in an entire document including a watermarked signature picture, or selecting a signature picture from a document displayed on a screen. In addition, the software can magnify a digital signature and digitize the signature and watermark and can transmit the signature to an ICD along with a command requesting signature authentication. Moreover, the software also enables the terminal to receive a document from an ICD for display. The software may also enable split windows so that a suspect document and a regenerated document can be viewed side-by-side to facilitate visual authentication. Furthermore, the software may be able to perform document comparison to identify document discrepancies.

To authenticate, the ICD is able to receive a watermarked signature from a terminal, remove the standard graphic watermark from the watermarked signature, generate a regenerated document from the remaining marked signature and transmit the regenerated document to the terminal for examination. An example of how a signature is authenticated is instructive.

After a physician gains access to a terminal via an ICD-terminal interrogation, the physician selects a review software application which allows the physician to select and examine one or more documents which were previously approved and stored on a server in the manner described above. After selecting the review application, the physician selects one document (e.g. patient record or check, etc.) to examine and, referring to FIG. 27, at block 701, the software displays the selected document, in HTML format as earlier stored. As part of the stored document, the software displays a digital and watermarked signature picture purportedly representing the signature of the physician who approved the document. The date and time of approval may or may not also be displayed. In addition, the software also provides an “AUTHENTICATE” icon adjacent the digital signature picture. It will be assumed that the reviewing physician is the physician who purportedly originally approved the document being examined and that the physician’s scripted signature picture, standard watermark and mark modifying program, all stored on the physician’s ICD, remain the same.

While the physician is reviewing the document, the physician notices something which the physician cannot remember approving. For example, while the document may indicate that eight capsules of drug A were administered to a patient the physician may clearly remember that only two capsules of another drug B were administered. While the physician recognizes that she may have made a mistake, the physician nonetheless would like to authenticate the document.

Referring again to FIG. 27, to authenticate the document, at block 703 the physician selects the AUTHENTICATE icon and the software recognizes the selection. At block 705 the software identifies the watermarked digital signature picture and isolates that portion of the displayed document. Next, at block 707 the terminal transmits an authentication request to the ICD along with the watermarked signature picture. At decision block 709 the terminal waits to receive a re-generated document from the ICD 10.

Referring also to FIG. 28, at block 801 the ICD receives the authenticate request and the watermarked signature picture. At block 803 the ICD retrieves the standard watermark and the physician’s digital signature picture from its memory. At block 805 ICD 10 removes the standard watermark from the watermarked signature picture thereby generating a watermark which specifically corresponds to document content. At block 807 ICD 10 expands the remaining content watermark into a re-generated document. The re-generated document includes the document which was originally approved by the specific instance of the physician’s digital signature picture and may include additional data if additional data was added to the approved document during standard watermark modification. At block 809 the ICD transmits the re-generated document to the terminal.

Referring again to FIG. 27, at block 709 when the regenerated document is received, control passes to block 711 where the terminal displays both the suspect and re-generated documents side-by-side for comparison. The physician should then be able to visually compare documents to determine if the documents are identical.

If desired, the terminal software can be equipped to itself compare documents to determine similarity. To this end, at block 713, the software compares the suspect and re-generated documents. In addition to comparing visual document information (e.g. text, graphics, data, etc.), the terminal software can also compare any additional data which was added to an original document to the additional data in the reGENER-
ated document. Thus, even hidden or visually meaningless (e.g. a bar having varying pixel intensities) random information can be used to authenticate an associated document.

[0282] Clearly, facilitating document comparison via software is advantageous for several reasons. First, as indicated above, random data comparison ensures a more thorough comparison. Second, presumably software comparison would be much faster than visual manual comparison. Third, for long documents such as a mortgage, contract, historical medical record, etc., software could compare every aspect and all document information to identify even a single document change.

[0283] Referring again to FIG. 27, where an original and a re-generated document are identical, the terminal indicates authentication at block 715. Where the documents are even slightly different the terminal indicates “no match” at block 717 signaling that the signature on the suspect document was not provided by the physician.

[0284] In another embodiment of the invention public key encryption (PKE) may be used with a digitally watermarked signed document to authenticate the document in the absence of a physician’s ICD. A conventional PKE system is described in U.S. Pat. No. 5,689,567 (hereinafter the “567 patent”) which has been referenced above and which is incorporated herein by reference. Generally, in a PKE system each system user has both a “secret key” and a “public key” for encryption purposes. To effectively mark a document for authentication purposes a mark (i.e. bar graph or seal, etc.) is generated by subjecting document content to the secret key. Thereafter the mark is applied to the document and can be stored or printed out on hard copy. To authenticate a marked document, if the document is a hard copy, the document is scanned into a computer to generate a digital document. After scanning or if the original document to be authenticated is a digital document, the mark is lifted from the digital document and used to regenerate a document corresponding to the mark using the public key of the person who supposedly approved the document via the mark. To this end, in a hospital facility, for example, all physicians public keys may be stored on an Intranet and may be accessible for authentication purposes.

[0285] After the public key corresponding to the physician who supposedly approved the document is used to expand the mark into a re-generated document, the original and regenerated documents are compared to authenticate. This type of PKE system can clearly be used with the present invention to generate documents from watermarks for authentication purposes.

[0286] Also, in accordance with the ’567 patent, a hashing method can be used to encrypt, decrypt and authenticate a document. To this end, according to the present invention, after a standard mark (e.g. a signature picture) is added to a document, document content or a representative portion thereof may first be hashed using a hashing code and generating an initial document hash. Thereafter, the initial hash may be encrypted using a private encryption key to generate a watermark which is applied to the document.

[0287] In this case, to authenticate, a watermark is identified on a document and is decrypted using a public encryption key to generate a re-generated hash. Next, a private key is used to again hash the document content generating a document hash. The document and re-generated hashes are thereafter compared to authenticate.

[0288] It should be appreciated that while the inventive time dependent electronic watermark described herein is extremely advantageous in the medical records area to authenticate an approval indication, clearly, this invention can be used in any application where a digital approval must be provided. For example, where bills are paid by electronic check, a users digital card time dependent watermark can be provided on the electronic check, the mark generated in the manner described above. Similarly, a digital time dependent watermark could be provided when a credit card number is used to purchase something over the Internet. In either of these two applications, instead of generating the watermark using an ICD, a terminal itself could be used to generate the mark and apply the mark to a terminal stored digital signature.

[0289] Referring to FIG. 29, an exemplary signature picture 949 is illustrated and includes a scripted signature picture 953 and a watermarked border 951. Referring also to FIG. 30, a watermarked signature picture 955 applied to an exemplary document 957 in a designated approval field (phantom identified by numeral 959) is illustrated. Picture 955 includes the signature picture 953 inside a watermarked border 622 digitally signed document 620 according to the present invention is illustrated. The exemplary document 957 is a digital prescription which includes information which one would expect to find on a prescription. The information includes a prescribing physician’s name and address 961, a patient’s name and address 963, and a prescription order 965 including medication prescribed, amount and required administration frequency. In this case, using a prescription software program, a physician fills in the information on the document 957 via a terminal. Assuming the information is accurate the physician then request a signature from the physician’s ICD 10 at which point the content of document 620 is transmitted to the ICD 10.

[0290] Referring again to FIG. 26, when the physician’s ICD 10 receives the document, assuming the document content DC is less than the threshold requirement TDC, ICD 10 adds random text/numbers to the DC. Thereafter, at block 656 the physician’s signature picture is added to the document, at block 658 the modified mark is generated, at blocks 659 and 660 the modified mark is used to modify the digital signature picture and at block 662 the document 957, with the watermarked signature picture, is transmitted back to the terminal for review and if signed properly, for further transmission to other network storage or processing devices.

[0291] After digitally “signing” the document 957, the signed document is displayed and then transmitted to a server. Thereafter, when the prescription is filled, the signed document can be electronically returned to the physician stamped “filled”. Then, to authenticate the prescription the authenticate process described above can be performed.

[0292] In addition, it should be recognized that while a signature block is very personnel to a user and therefore is preferred in the present invention to convey a feeling of responsibility for the document to which the block is ascribed, any type of personal identifier which can be pictorially represented may be marked using a content dependent electronic watermark. For example, even a single horizontal line could be watermarked. Moreover, other types of information could be marked with time dependent watermarks for authentication purposes. For example, a video clip could be so watermarked, an audio clip could be so watermarked and so on. Furthermore, an electronic watermark can take any of several different forms such as, for instance, providing the background to a signature field or indeed providing the background for an entire document. In the case where the mark
comprises the entire document background the entire background would have to be used during authentication to regenerate the document.

Moreover, while the watermarking procedure has been described as one wherein an entire document content is used to generate a mark, in the alternative a document digest may be used instead. For example, referring again to FIG. 29, a digest may simply include information filled in on a check such as issues, date, amount and signature where a digest is used to generate a watermark, comparison to authenticate copies only digest information, not an entire document.

While the approval/authentication concepts of the present invention were described above in the context of an ICD, the invention should not be so limited and is meant to cover other embodiments. The most general aspect of the approval/authentication concepts is that a document which has been approved by someone can be authenticated by using the document content. Other examples of how this general concept can be implemented are helpful to understanding the full import of this invention.

For example, according to another embodiment of the invention, a physician’s terminal may be equipped with both a scanner and a printer and, where the terminal is personal to the physician, the terminal may share the physician’s private secret encryption key, the physician’s public encryption key accessible via a LAN or the like, to other facility personnel.

In this case, if the physician has a hardcopy paper document which she would like to endorse, the physician may sign the paper document via a pen and a handwritten signature. Then the signed document is scanned into the computer via the scanner. Thereafter, it is envisioned that the processor retrieves the physician’s private key, applies the private key to the document content (including the signature) to generate a watermark and then applies the watermark to a digital representation of the document. Thereafter, the digital representation may be printed out including the watermark or, in the alternative, the originally hand signed document may be provided to the printer input and run through the printer to add the watermark to the originally signed document. In effect, the printer would only print out the watermark which would be applied to the signed document.

Subsequently, to authenticate the document the watermark is identified on the document and scanned back into a terminal, the public key corresponding to the physician’s signature which appears on the document is retrieved and is used to decrypt the watermark thereby generating a complete copy of the document which could either be examined on a computer display or printed out on hard copy for comparison to the original document. According to yet another embodiment of the invention, a physician’s terminal may be equipped with a digital signature pad for providing a digital signature. Digital signature pads are well-known and have been extensively used in the credit card industry to digitally record purchaser’s signatures. A typical pad includes a flat sensing surface which senses the position of a pen tip as the tip is moved along the surface and generates a position signal indicating tip position. The position signal is provided to a computer which thereafter generates a “picture” of the pen tip movement. Where the pen is used to script a signature, the picture generated by the computer is the scripted signature. In this case, it will also be assumed that the physician’s private key is stored on a private terminal and public key is generally available.

In this case, assuming a document is displayed on a computer display screen which a physician would like to approve, it is envisioned that the physician selects an approve icon on the display. Thereafter, the computer terminal requests the physician to hand script a signature on the digital pad. As the physician hand scripts the signature on the pad, the computer provides a digital representation of the signature in an approval field on the displayed document.

After the signature is completed, the computer retrieves the physician’s private key, encrypts the signed document using the private key and thereby generates a watermark and applies the watermark to the displayed document, the mark remaining with the document when stored or printed out. Authentication in this example is the same as in the previous examples.

VIII. EXAMPLES

A few examples of how the present invention is intended to operate are instructive and aid in an understanding of why the invention is extremely advantageous. In each of the first four examples below, it will be assumed that both Penicillin and Tylenol are to be administered to a single patient within a facility within a specific time period and in specific doses by one of several authorized physicians. The patient is wearing an electronic identification bracelet like bracelet 40 of FIG. 2 which has, in its memory, at least some and perhaps all of the information which is illustrated in FIG. 9.

Example 1

In a first example, it will be assumed that a physician’s ICD 10 is relatively complex so that the ICD 10 itself is capable of recognizing different types of received information, building a server target address for the received information and providing configuration information for displaying the received information via a web browser on a display 103. Initially, referring also to FIG. 6, it will be assumed ICD 10 includes a physician identifying segment in memory 262 which identifies the physician associated with the ICD 10.

In this case, initially, it will be assumed that two Penicillin capsules and a single Tylenol capsule are dispensed into a container like container 200 illustrated in FIG. 5. In addition, referring to FIG. 10, a programming device such as dose dispenser 150 (see FIG. 7) provides a dispensation to processing device 75", device 75" storing received information in its memory. Moreover, dose dispenser 150 also generates a dispensation address for storing record 340. An exemplary dispensation record address 400 is illustrated in FIG. 13. Address 400 includes a field indicating the facility at which dispensation occurred (e.g. “St. Mary, Springfield”), a descriptor field (e.g. “medication”), an event field (e.g. “dispensed”), a patient ID field (e.g. “0987654321”), a date field (e.g. “May 19, 1996”) and a time field (e.g. “13:42”). All of the fields in address 400 are generated by dispenser 150.

As the physician makes her rounds, the physician eventually visits the patient for which the Penicillin and Tylenol were dispensed. After an abbreviated examination, the physician elects to administer half (i.e. 1 capsule) of the dispensed Penicillin and the entire dose of dispensed Tylenol (i.e. 1 capsule) to the patient. To administer the drugs the physician must first gain access to the Penicillin and Tylenol by unlocking container lid 204. In this example, it will be assumed that processing device 75" maintains lid 204 locked.
until a specific set of information is received by device 75" which matches information stored in the memory of device 75". Specifically, both patient identifying information which matches similar information in FIG. 10 and physician identifying information which matches similar information in FIG. 10 must be received by device 75"

[0304] Thus, to gain access to the contents of container 200, the physician places container 200 proximate the patient’s bracelet 40 and causes the patient’s bracelet to transmit patient identifying information (e.g. the patient identification number) to transceiver 81" on device 75”. In this example this is accomplished by pressing an activation button (not illustrated) on device 75" in FIG. 2. A short time thereafter, the physician places container 200 proximate ICD 10 and causes ICD 10 to transmit physician identifying information to transceiver 81" by pressing button 18.

[0305] When device 75" receives the patient and physician identifying information, device 75" compares the received information with similar information stored in the memory of device 75". Where the received and stored information is not identical, device 75" maintains lid 204 locked and may indicate a mismatch by generating an audible sound via device 87". However, if the received and stored information is identical, device 75" allows lid 204 to be opened by pressing button 228. Device 87" may generate a different audible sound indicating the match. Audible alerting device 87" may also serve to remind a physician when it is time to administer the enclosed treatment.

[0306] In addition to facilitating opening of lid 204, when button 228 is pressed device 75" transmits all of the information illustrated in FIG. 10 as an information segment to ICD 10. This transmission can be in any form which is recognizable by ICD 10. When ICD 10 receives the information segment, ICD 10 does several things. First, referring also to FIG. 6, processor 250 identifies the time at which the information segment was received and hence the time at which lid 204 was opened via clock 254, processor 250 storing the identified time as a time stamp segment. Here, it is assumed that medicine administered to the patient is administered a short time after lid 204 is opened and therefore, administration time is indicated by the time stamp segment. Second, processor 250 recognizes the received information segment as a medication administration record and therefore automatically formats the received information and the time stamp segment as an information packet like the medication administration packet illustrated in FIG. 14A.

[0307] In addition, ICD 10 uses received information to formulate a target address. To this end, in FIG. 14A, an exemplary target address is identified by numeral 444. Address 444 includes a facility field which indicates the same facility as the dispensing facility (i.e. St. Mary, Springfield, see also FIG. 13A), a descriptor field (i.e. medication), an event field (i.e. ”given"), a patient ID field (i.e. "987654321") and date and time fields (i.e. "May 19, 1996" and "13:42", respectively).

[0308] After lid 204 is opened, the physician removes a single Penicillin capsule and the Tylenol capsule leaving the second Penicillin capsule in container 200 and administers the removed capsules to the patient. The physician recloses lid 200 which again locks and is routed back to the pharmacy for reinventory. If desired, the physician may make a manual note indicating that only one Penicillin was administered (e.g. via dictation).

[0309] After the physician completes her rounds, it will be assumed that the physician’s ICD 10 includes ten information packets, each of which is similar to packet 440 in that each packet includes configuration information, a specific target address and some description information which describes a medical event (e.g. patient identifier, physician identifier, medication identifier, administration date/time, medication amount, etc.). In addition to the ten information packets, it is assumed ICD 10 forms an initial screen packet which summarizes ten information packets and provides interaction icons to facilitate physician review of the information packets. Referring to FIGS. 1 and 3, to transfer the initial screen packet and the information packets to system 194, the physician first gains access to a terminal 60 in one of the manners indicated above which is supported by the terminal 60. For example, the physician may position her badge proximate input device 64 at which time device 64 and terminal 60 generally interrogate ICD 10 to determine if the physician associated therewith is authorized to access the terminal 60.

[0310] After the physician gains access to terminal 60, the physician again positions ICD 10 proximate input device 64 and causes ICD 10 to transmit all ten information packets to terminal 60 via device 64. When the packets are received, browser 115 displays a full terminal screen which is configured in accordance with the instructions provided in the initial screen packet. To this end, the initial screen indicates the number of information packets received and also displays the interaction icons. The interactive icons are assumed to be REVIEW and STORE icons.

[0311] It is contemplated that a first physician might collect information packets via a first ICD 10 and a second physician might access a terminal 60 via a second ICD 10 to review, modify and approve descriptive information in information packets associated with the first ICD 10. Thus, after gaining terminal access via the second ICD 10, the information packets in the first ICD 10 are transmitted to the terminal 60 for review. In this regard, the terminal 60 may, after being accessed and receiving information packets, either allow the second physician to review, modify and approve the packets or may block the second physician from one or all of the review, modifying and/or approval abilities.

[0312] In most cases, it does not make sense for a physician who did not perform an examination to review, modify and approve information packets as the second physician likely would not know the specifics of an examination. For example, in the present case where a first physician elected to administer only one of two dispensed Penicillin capsules, the second physician would have no way of knowing that the first physician changed the prescription. Thus, if the second physician approved the information packet which indicates two Penicillin capsules were administered, the stored data would be erroneous.

[0313] To determine if a terminal accessing physician is the same physician who acquired information packets, the terminal 60, when accessed stores an accessing physician identifier. Then, when information packets are received from a second physician’s ICD 10, terminal 60 identifies the administering physician associated with the packets (e.g. the physician associated with the second ICD) and stores an administering physician identifier. Next, terminal 60 compares the accessing and administering physician identifiers, where the accessing and administering physician identifiers are identical, terminal 60 allows information packet review as described hereinafter.
However, where the accessing and administering physician identifiers are not identical, terminal 60 may do one of several things first. First, terminal 60 may simply indicate that the accessing physician cannot review, modify or approve the information packets and thereafter may terminate access to the terminal 60.

Second, terminal 60 may allow the accessing physician to review the information packets but may not facilitate modification and approval functionality. Restricting the accessing physician in either of these first two ways goes a long way to ensure that information transmitted to long term storage truly reflects an associated medical event.

Third, terminal 60 may add the accessing physician identifier to the descriptive information in the information packet and thereafter allow the accessing physician full review, edit and approve abilities. Then, when the descriptive information is stored, the accessing physician identifier is included therewith so that a complete audit trail for each information packet is formed. In addition, if desired, terminal 60 may also maintain an unmodified information packet for storage with each information packet which is modified by an accessing physician who is not an administering physician. In this manner, if modified descriptive information is erroneous, a record of unmodified descriptive information can still be accessed for review.

Continuing, assuming the physician elects to review the descriptive information in the information packets and is authorized to review, modify and approve packets, the physician selects the REVIEW icon. It will be assumed that the initial packet to review is the medication administration packet described above. When the physician selects the packet, browser 115 configures the browser screen as indicated by the configuration information stored in the packet and displays the descriptive information. In addition, browser 115 displays hyperlinks in instances when the configuration information so instructs and displays a hyperlink for the APPROVAL icon which indicates the target address. Thereafter, the physician can modify displayed information and then approve the information by selecting the APPROVAL icon.

In the present example, the physician consults her hand written notes and confirms that only half of the dispensed Penicillin was administered. Because the physician changed the amount of Penicillin administered to the patient from two capsules to one, the physician must modify the penicillin dose which is displayed. To do this the physician selects the dose amount which causes a pull down menu to open up providing the physician with other options (e.g., 1.5 capsules, 1 capsule, etc.) The physician selects one of the other options (i.e., in this case 1) and the menu closes as the dose amount is modified.

When the APPROVAL icon is selected, browser 115 transmits the approved information and associated hidden information to the server target address associated with the APPROVAL icon. After the first packet information has been approved, preferably the browser automatically presents the information in the next consecutive information packet via display 103. Again, the physician can quickly review the information, modify the information if necessary and approve the information for storage.

Thus, it should be appreciated that, using the inventive ICD 10 to collect information, configure browser screens and provide server target addresses for collected information streamlines the information gathering process and also streamlines the process of downloading information from such a device to a terminal for viewing, modification and approval.

In addition, by adding physician identification information to an information packet a record of medical administration information is formed. Moreover, by requiring an authorized physician to approve descriptive information which characterizes a medical event and identifying the approving physician in the descriptive information prior to long term storage, not only is the information review process easier and therefore more likely to be completed, the review process figuratively assumes "ownership" of approved data to the approving physician, thereby adding import to the approval process. In addition, by adding approving physician identification to the descriptive information or by adding a physician's watermarked digital signature to record, a complete audit trail for descriptive information is provided.

B. Example 2

In this second example, it will be assumed that a physician's ICD 10 relative is relatively simple in that the ICD 10 cannot itself formulate target server addresses or HTML configuration information and cannot generate most descriptive information (e.g., date and time stamp segments). Instead, in this example, address, configuration and most descriptive information is provided to ICD 10 by other system devices.

In this example, like the preceding example, it will be assumed that two Penicillin capsules and a single Tylenol capsule are dispensed into a container like container 200. However, in this case, in addition to providing the information illustrated in FIG. 10, dose dispenser 150 includes a specifier apparatus (see 64 in FIG. 3) which also provides a server target address and browser screen configuration information in HTML code to container device 75" (see FIG. 5). For example, referring again to FIG. 14A, in this example, virtually all of the HTML code illustrated, including format field information, would be provided by dispenser 150 except for descriptive portions of some fields. Thus, for example, in field 444, the portion which reads "given" along with the patient identification number, date and time, would not be provided. Similarly, in field 452, verification "YES" would not be provided. Moreover, the administering physician in field 464 would not be provided.

To form the incomplete packet, dispenser 150 may be equipped with special software for generating appropriate HTML code or, in the alternative, dispenser 150 may be linked to a server for generating the HTML code. Referring to FIG. 7, in the present example, it is advantageous if dispenser 150 is linked to pharmacy server 186 for receiving pharmacy information related to ordered prescriptions. In addition, by being linked to the pharmacy server 186, when ICD 10 returns information to server 186 after dispensation and approval, dispenser 150 may access the returned information to confirm dispensation and if dispensation did not occur or a prescription was changed, dispenser 150 may indicate so via an alarm or some form of quality control reporting.

As in the previous example, when Penicillin and Tylenol are placed inside container 200, container 200 is positioned proximate a transceiver associated with dispenser 150 and dispensation information is transmitted to container device 75" via the dispenser specifier apparatus or output device 64 (see FIG. 3). In this case, however, transmitted
information includes the entire packet 440, less the descriptive information (e.g., receiving patient i.d., date, time, administering physician, etc.).

[0326] Again, it is assumed that when the physician visits the patient for whom the Penicillin and Tylenol were dispensed, the physician elects to administer only one capsule of each of Penicillin and Tylenol. Once again, to gain access to the capsules, the physician performs a specific procedure to open lid 204 whereby device 75° receives patient and physician identifying information, compares the information with similar information stored in the memory of device 75° and facilitates unlocking of lid 204 only when there is a precise information match.

[0327] In addition, if a precise information match occurs, referring again to FIG. 14A, device 75° fills in various blank portions of packet 440 including verification field 452. It is assumed that when lid 204 is unlocked, drugs therein are administered to the patient associated with the patient identification number which was received by device 75°. Therefore, device 75° fills in the patient identification number in field 444 further defining the target address. It is also assumed that the physician who opens lid 204 administers the drugs and therefore physician identifying information is filled in field 464.

[0328] After lid 204 is unlocked, when a physician presses button 228 to open lid 204, device 75° identifies the current date and time and provides that information both in the target address (field 444) and in field 468 (i.e. the time stamp). At this point packet 440 is complete as illustrated in FIG. 14A.

[0329] Assuming device 75° is proximate the physician’s ICD 10, once packet 440 is complete, device 75° transmits entire complete packet 440, including HTML code specifying target addresses and screen configuration, to ICD 10. When ICD 10 successfully receives an information packet, ICD 10 may generate an audible signal or a visual signal (e.g. activate an LED to indicate successful reception). ICD 10 simply stores packet 440 until caused to transmit packet 440 to a terminal 60 for review, modification and approval.

[0330] The remainder of this example, is similar to the example above. Thus, after her rounds, the physician accesses a terminal and downloads information packets to a browser for review, modification and approval prior to storage.

[0331] This second example is advantageous because ICD 10 and other smart devices (e.g. container 200) need not be able to facilitate complex computations and formatting procedures. Instead, ICD 10 and smart devices, at most, must fill in a few descriptive fields and basically act as information storage buffers. In addition, this second example is advantageous because a dispenser 150 can specify a target address for returned information and how information which is returned to a terminal should be configured for review. This should facilitate a more flexible system. Moreover, the ICD 10 and other smart devices are relatively inexpensive as less remote computing power is required.

[0332] In addition, in this second example, as indicated above, dispenser 150 can close the information loop by tracking information returned to the pharmacy server 186 via ICD 10 and comparing that information to prescriptions which were to be administered. To this end, in addition to including the components illustrated in FIG. 3, the dispenser processor also includes a clock (not illustrated). In addition to indicating medication to be dispensed each prescription includes a prescribed administration period such as “between 2-3 PM” which is accessed by the dispenser 150 processor for each drug dispensed. When the drug is dispensed, the processor identifies the required administration period. For each prescription, at the end of the administration period or at the end of some predetermined reporting period (e.g. 2 hours) following the end of an administration period, the dispenser processor retrieves any data corresponding to a specific prescription which was returned by an ICD and also recognizes the absence of such data.

[0333] Where no data for a specific prescription has been provided by an ICD, the dispenser 150 may do any of several different things. First, the dispenser 150 may indicate via a dispenser display (see 103 in FIG. 3) that administration, potentially was not performed. In addition, dispenser 150 may also periodically generate an audible “chirp” via indicator (i.e. alarm) 111. In the alternative, some other indicating mechanism such as an e-mail or pager signal may be generated to inform a physician or attending nurse of a potential mismedication. Still further, the dispenser processor may simply generate a record indicating possible mismedication. Subsequently, if ICD prescription data for the specific prescription is provided the indications may be automatically halted.

[0334] At the end of a prescribed administration or reporting period, if data for a specific prescription has been provided the dispenser 150 may retrieve the data and compare the data to the original prescription. In the present case where the administered medication was modified and therefore does not match the prescription exactly, it is contemplated that dispenser 150 generates a prescription/administration (P/A) quality control modification report indicating that the drugs administered were in fact different than those prescribed. In addition the P/A report may also indicate matching prescriptions and administrations.

[0335] The dispenser reports may be provided to an attending pharmacist for daily or weekly review or to a physician for review or indeed to an administrator or the like to track administration efficiency and accuracy.

C. Example 3

[0336] In this third example, it will be assumed that an ICD 10 is a hybrid of the ICDs in the above examples in that each ICD has less computing ability than the ICDs in the first example and more computing ability than the ICDs in the second example. In this example, it will be assumed that some of the HTML code for configuring a browser and providing browser addresses is provided to ICD 10 and that ICD 10 generates the remainder of required information and at least some of the descriptive information.

[0337] In this example, like the preceding examples, it is assumed that two Penicillin capsules and a single Tylenol capsule are dispensed into a container like container 200. In this example, dispenser 150 provides an HTML dispensation information packet in HTML to device 75° which includes information for configuring browser 115 screens to indicate dispensation information. To this end, referring to FIG. 13B, an exemplary dispensation information packet 404 is illustrated. Referring also to FIG. 13C, a browser screen 412 which corresponds to packet 404 is illustrated including hypertext links 416 and 420, respectively, to a patient’s demographic record and the bibliographic record of the physician who dispensed the medication. Packet 404 is formatted according to HTML and uniform resource locator (URL) conventions. FIG. 13C illustrates the medication dispensation record 404 as it is displayed by a browser 412, FIG. 13A
illustretes the URL 400 generated for the medication dispensation record 404 which identifies the location at which it is or will be stored.

[0338] In this example, prior to dispensing a dose to a container 200, a physician reviews dispensation information via screen 412. If dispensation information is correct, the physician approves the information and packet 404 is transmitted to container 200.

[0339] Again, it is assumed that when the physician visits the patient for whom the Penicillin and Tylenol were dispensed, the physician elects to administer only one capsule each of Penicillin and Tylenol. Once again, to gain access to the capsules, the physician performs a specific procedure to open lid 204 whereby device 75" receives patient and physician identifying information, compares the information to similar information stored in the memory of device 75" and facilitates unlocking of lid 204 only when there is a precise information match.

[0340] As in the first example, when button 18 on ICD 10 is pressed, ICD 10 identifies the time and date and stores that information as a time stamp segment for placement in a subsequently formed information packet.

[0341] After lid 204 is unlocked, when a physician presses button 228 to open lid 204, assuming device 75" is proximate the physician’s ICD 10, device 75" transmits packet 404 (i.e. the HTML dispensation information packet in FIG. 13B) to ICD 10. When ICD 10 receives packet 404, ICD 10 modifies packet 404 by adding descriptive information, additional browser screen formatting information, formulating a specific target address and providing configuration information for interaction icons as indicated above, thereby generating a completed information packet like exemplary packet 440 in FIG. 14A.

[0342] The remainder of this example, is similar to the examples above. Thus, after her rounds, the physician accesses a terminal and downloads information packets to a browser for review, modification and approval prior to storage.

D. Example 4

[0343] In this fourth example, it will be assumed that all smart devices and the ICD 10 are extremely simple in that none of the devices is capable of formulating or storing complex and complete screen configuration information. Instead, it is assumed that target address and minimal configuration information is provided to the smart devices and ICD 10 by other system devices and that the smart devices and ICD 10 simply provide descriptive information during a patient visit. In this example, to facilitate information review, a simple software package is provided on each terminal 60 which receives the minimal configuration information, correlates the minimal configuration information with a more detailed configuration format, and provides the detailed format for browser configuration control.

[0344] In this example, as in the second example above, dose dispenser 150 provides a server target address and browser server configuration information to a smart container device 75" when Penicillin and Tylenol are dispensed into a container 200. However, unlike in the second example where screen configuration information is provided in HTML code, in this example a simple configuration indicator code is provided which can later be expanded into more detailed HTML code for configuration. For example, the simple configuration indicator may be as simple as a single character or number. In this case, assuming there are only ten possible screen configurations for viewing descriptive information packet information, each of the ten possible configurations is associated with a different number indicator 0 through 9. In the present example, it will be assumed that a screen configuration for reviewing descriptive information in a medication administration information packet is identified by number indicator 4. In this case, in addition to receiving a target address upon medicine dispensation, container device 75" also receives indicator 4 which is stored for later transmission to ICD 10.

[0345] When lid 204 is unlocked so that the physician can administer the medicine therein, device 75" identifies descriptive information and provides the descriptive information, target address and screen configuration number indicator (i.e. “4”) to ICD 10. ICD 10 stores the received information as a packet until caused to transmit the packet to a terminal 60.

[0346] In addition to storing the described information packets, it is also assumed ICD 10 also generates a dynamic initial screen indicator to provide dynamic information to browser 115 for display via the initial screen. To this end, it has been recognized that generally the initial screen will often include essentially the same information. For example, a typical initial screen will often only include an indicator to identify the number of files to be reviewed and perhaps a small number of indicators indicating the types of files to be reviewed (e.g. billing, dispersion, monitored information, dictation, etc.). Assuming a simple initial screen which only displays the number of files to review and icons to select review or store options, the dynamic initial screen indicator is simply a number. Assuming 10 files are stored in an ICD after a physician makes her rounds, the screen indicator is 10.

[0347] After the physician completes her rounds, the physician gains access to a terminal 60 in the manner described above. After the physician gains access and activates ICD 10 to transmit stored data to a terminal 60, ICD 10 transmits the initial screen indicator (e.g. 10) and the information packets.

[0348] When the transmitted information is received, terminal processor 107 performs several functions. First, processor 107 dissects each information packet thereby identifying, with respect to each packet, a target address, descriptive information and the screen configuration number indicator. Processor 107 uses the number indicator to identify a screen configuration for displaying associated descriptive information and forms an HTML packet like 440 (see FIG. 14A) for each received packet, filling in descriptive information where appropriate. Each HTML packet is then stored in RAM 109.

[0349] Second, processor 107 identifies the initial screen indicator and fills in an appropriate field in an initial screen configuration. Then the initial screen is configured to enable a physician to review the descriptive information packet information. In the present example, because the initial screen indicator is 10 (e.g. there are 10 files to be reviewed), the initial screen indicates “There are 10 files to review” and provides REVIEW and STORE icons.

[0350] The remainder of this example is similar to the examples above. Thus, the physician can review, modify and approve information in each file stored in RAM 109.

[0351] This embodiment is advantageous in that most of the formatting capability can be provided in a terminal 60 as opposed to an ICD 10 as other smart devices. This is advantageous as it is contemplated that, in a typical facility, there will be many more ICDs and smart devices than there will be
terminals 60. Nevertheless, consistent with the present invention, this embodiment still has the advantage of specifying target addresses via an ICD 10, instead of a server and specifying browser screen configuration albeit in an abbreviated format.

E. Example 5

[0352] In this fifth example, instead of interacting with a smart container 200, referring to FIGS. 1 and 4, it will be assumed that a smart IV treatment device 116 which, in addition to including an IV pump and proper patient linkage hardware, includes the hardware illustrated in FIG. 19, is provided in a patient’s room 104. In addition, it will be assumed that the patient has been linked to the IV pump for several days and that a physician visits the patient’s room to monitor patient condition and generate a report every 4 hours. Thus, a new patient record is generated every four hours.

[0353] In this example, as in the second example above, it will be assumed that ICD 10 is relatively simple in that most data is collected from IV device 116, and not generated. To this end, in addition to providing a dispensation information segment record indicating medicine dispersion since the most recent data acquisition (e.g. four hours earlier), device 116 also generates a target address for the dispensation record and browser screen configuration information indicating how a browser screen should be configured for data review. The dispensation information segment and address are assembled into an HTML information packet which includes several incomplete descriptive fields including a patient ID field, a time and date field and a physician ID field.

[0354] When a physician visits the patient linked to device 116, the physician establishes a patient association with ICD 10 as indicated above, the patient association stored as a packet identification segment. After the patient association has been established, the physician causes device 116 to transmit the incomplete packet to ICD 10.

[0355] When the incomplete information packet is received, if the time is not already identified in the received information, ICD 10 identifies the time and date of receipt. ICD 10 places the time and date of receipt, patient identifying information indicating the patient who received the IV medication (i.e. patient identified in the patient identification segment) and physician identifying information indicating the physician with whom ICD 10 is associated, in appropriate information packet fields thereby completing an HTML packet similar to packet 440 illustrated in FIG. 14A.

[0356] A typical IV packet might include a period indicator which indicates the monitored time period (e.g. previous four hours) which corresponds to the dynamic data in the packet and a delivery rate field which indicates the rate of medicine delivered by IV device 116. Where the delivery rate changed over the most recently monitored time period, the delivery rate field may include several medicine rate indicators which are each correlated with a delivery period over which the specific rate was provided. In the alternative, the rates may be provided in other forms such as a graph of rate versus time. In addition, the IV packet will also include a medication field indicating the medication dispensed via the IV, the physician who authorized the medication, the patient name and so on. Further more, the IV packet will also include a physician identifying field indicating the physician who acquired the IV packet.

[0357] As in the previous examples, when a physician completes her rounds, the physician gains access to a terminal 60 and transfers information packets, including the IV packet, to the terminal browser 115. Once again, the receiving browser identifies initial screen configuration information indicating the number of files transmitted to terminal 60 and displays the initial screen, including REVIEW and STORE icons.

[0358] Assuming the physician selects the REVIEW icon, terminal 60 displays the first information packet in the associated configuration format. As above, the IV information is displayed for review, in a format which is specially configured to display IV information. Although editing tools for modifying displayed IV information may be provided, such tools probably would not be provided as the IV information simply reports actual medicine administration and could not have been modified by a physician arriving for a visit after administration occurred. An APPROVAL icon allows the physician to approve the IV information for storage at the target address.

[0359] While this smart IV example is relatively simple, this example illustrates that the invention may be used with any type of smart device to remotely collect data and generate an ultimate target address and screen configuration data. The important aspect of a smart device is that the device can monitor some quantifiable information which is associated with a patient and which is advantageous to collect and store for later retrieval.

F. Example 6

[0360] Referring again to FIG. 1, in this sixth example of how the present invention might operate it will be assumed that a physician’s ICD 10 is equipped to receive audio information (e.g. voice) via digitizer 22 when dietation button 26 is pressed. Thus, during a patient visit, a physician may use ICD 10 to take audio notes.

[0361] To this end, at the beginning of a patient visit, a physician’s ICD 10 identifies the patient by communicating with the patient’s bracelet 40 (see FIG. 2) and, after forming a patient association, stores patient identifying information as a patient identification segment. In addition, ICD 10 also stores a physician identification segment indicating the physician associated with the ICD. When the physician wants to form an audio note, the physician presses button 26 and thereafter speaks in the vicinity of digitizer 22.

[0362] When button 26 is pressed, ICD 10 recognizes that audio information is to be received and performs several different functions. First, ICD 10 automatically generates a target address for audio information to be received. The target address specifies a server used by a facility transcription pool. The transcription pool server is where all digital dictation is stored which is then transcribed either manually by facility personnel or automatically by transcription software. For the purpose of the present invention it will be assumed that transcription is manual.

[0363] In addition to generating the target address, ICD 10 identifies the time and date which are stored together as a time stamp segment. Moreover, ICD 10 automatically generates an incomplete audio information packet including browser screen configuration information and time, patient identifying and physician identifying fields and fills in the time and identifying fields with information from the time stamp, patient identifying and physician identifying segments. The only field which is not completed in this example is an audio dictation field which is to receive the digital audio information upon reception. In addition to generating the packet described above, the ICD 10 may also generate browser for-
matting information to formulate specific types of templates to be filled in by a member of the transcription pool. For example, the templates could include a template for a typical patient visit, a template for a prescription to be filled and so on. After the audio information packet is formed, ICD 10 stands ready to receive audio information via digitizer 22.

With button 26 pressed, when the physician speaks within the vicinity of digitizer 22, digitizer 22 receives the dictation, digitizes the dictation and stores the digitized information in the audio dictation field. At the end of the dictation, the physician stops pressing button 26. In the example, if, prior to ICD 10 forming a new patient association, the physician again presses button 26 to dictate again, the subsequent dictation is stored in sequence at the end of the audio dictation field. Once a new patient association is formed, when button 26 is pressed, a new audio information packet is generated.

In the case of an audio information packet, among other things, the configuration information will configure a browser screen which identifies time and date of dictation, dictating physician and patient visited. In addition, the configuration information may also provide interaction icons to allow a reviewing physician to play back and perhaps edit dictation. For example, interaction icons may include “PLAY”, “STOP”, “REWIND”, “ERASE”, “FAST FORWARD” and so on.

After a physician completes her rounds, as in the previous examples the physician gains access to a terminal and transmits an initial screen configuration packet and other information packets, including the audio information packet described above, to the terminal. Browser 115 receives all the packets, stores the information packets and configures the initial browser screen as instructed by the initial screen configuration packet.

As the physician reviews the information packets, eventually the physician selects the above audio information packet for review. When the audio information packet is selected, browser 115 displays the descriptive information in the audio information packet including the interaction icons. The physician can review the audio information packet via the icons and, if necessary, may correct the dictation via some suitable means (not illustrated).

A second dictation facilitating ICD 201 is illustrated in FIG. 20. ICD 201 is similar to a conventional digital dictaphone in that ICD 201 is a hand held device including an audio digitizer 203, a speaker 205 and conventional editing buttons, “Play” 207, “Record” 209, “Reverse” 211, “Fast Forward” 213 and “Stop” 215. In addition, however, ICD 201 includes a transceiver 217, target address specifying or indicating buttons “Pharmacy” 219, “Billing” 221, “Personal” 223 and “Transcription” 225, a processor 250 (see FIG. 6) which is capable of configuring target addresses and screen configuration information and is capable of generating some descriptive information (e.g. physician identifying information, time and date, etc.). An optional screen 231 for viewing either collected data or a target address may also be provided.

With an ICD like ICD 201, it is envisioned that, by selecting one of the specifying buttons 219, 221, 223 or 225, a physician can generally select the target address for subsequent dictation. In addition, as with a conventional dictation device, by providing editing buttons on ICD 201, a physician can correct dictation immediately if desired.

When a physician stops to visit a patient during her rounds and would like to dictate a note which should be provided to a specific facility department, the physician first selects an appropriate department for receiving the note. For example, if the note is for the pharmacy to prescribe a specific medicine for a patient at a specific time, the physician presses button 219. When button 219 is pressed, ICD 201 generates an incomplete audio information packet which specifies, in appropriate fields, a visited patient, a visiting physician, time and date and a target address which specifies the pharmacy server. Once again, the only field which is not filled is the audio information field. Thenceforth, the physician uses editing buttons 207, 209, 211 and 215 to dictate an intended note which is digitally recorded in the audio information field.

After her rounds, the physician accesses a terminal, transmits information packets and edits and approves the packets. With respect to the audio information packet targeting the pharmacy server address, when the audio information is approved, instead of going to the transcription pool, the information is transmitted to the pharmacy server.

In the alternative, ICD 10 may be configured such that more than a single server address can be selected by consecutively pressing more than one button 219, 221, 223 or 225 or, so that all dictation, in addition to being provided to the selected server, is also provided to the transcription pool server (or some other server for that matter).

G. Example 7

In this seventh embodiment of the present invention, in addition to collecting audio information and other information which is provided by other smart devices (e.g. patient ID number, dispensed drug type and amount, etc.) an ICD is equipped to collect video information. To this end, referring to FIG. 21, an exemplary video equipped ICD 301 includes a main body housing in which a processor and other already described hardware (see FIG. 6) is housed. Most importantly, the other hardware includes a clock and a memory (both audio, video and other information) in which user identification information is stored. In addition, ICD 301 includes conventional video editing buttons “Play” 305, “Record” 307, “Reverse” 309, “Fast Forward” 311 and “Stop” 313 which are linked to the ICD processor to facilitate recording, reviewing and erasing of video and audio information.

Moreover, ICD 301 also includes a video lens 315, a video viewer 317 which is pivotally attached to housing and an audio digitizer (e.g. digital microphone) 319 for detecting audio signals. As with all ICDs described herein, ICD 301 also includes a transceiver which can both receive information from smart devices and transmit information to smart devices and to a terminal. In addition, other data collecting devices may be provided such as a bar code reader.

Furthermore, ICD 301 also includes a toggle button 325. It is envisioned that, as with the audio ICD illustrated in and described with reference to FIG. 20, ICD 301 may be used to select a specific facility department to which collected data (e.g. video and audio) should be provided. In this example, the capabilities of viewer 317 are used in conjunction with toggle button 325 to select specific target facility departments. To this end, it is envisioned that where no other server is selected, a facility video archive department and associated server are selected as a default target for the purposes of generating a target address for collected information. Thus, if a user does not select a different target server, ICD 301 generates a target address specifying the archive server.
To select a different target server, a user looks into viewer 317. At the bottom of a displayed screen, a server indicator is displayed, the currently selected target server specified therewith. Thus, initially the server indicator indicates “Archive Server”. To select a different target server, the user depresses button 325 once which causes the server to change and causes the server indicator to also change accordingly. For example, pressing button 325 once may change the server indicator from “Archive Server” to “Pharmacy Server”. By pressing button 325 a second time the server indicator observable through viewer 317 again changes to indicate another possible target server (e.g. “Billing Server”). Where there are five possible servers, any of the five servers can be selected by releasing button 325 once the desired server is indicated by the server indicator. To return to the initial default “Archive Server”, the user simply scrolls through the server choices and, after the last choice has been displayed, the next time button 325 is pressed, the default server is again selected.

In addition, it is envisioned that, in addition to enabling selection of a specific target server, one choice provided by toggle switch 325 should be “No server” so that while information can be collected, no server has to be selected during data collection. Then, if the user desires, the user may, while reviewing a video clip via viewer 317, select any portion of the clip for delivery to a specific server.

Two examples of how ICD 301 might operate are provided hereinafter. In a first example, in a medical facility, when a physician makes her rounds and visits a patient, ICD 301 can be used as described above with respect to the preceding examples to establish an association with a specific patient through any of several different interrogation protocols. After association has been established, ICD 301 begins to build a conventional target server address using the physician’s ID information, patient ID information, time and date (from the ICD clock, not illustrated). In addition, if IV information or drug dispensing information is collected, that information is automatically formatted for subsequent delivery to a terminal for viewing and further delivery to an appropriate server address indicated by the target address.

Assuming some peculiar visible symptoms are observed, the physician can use ICD 301 to record video of the symptoms for archiving and subsequent diagnosis. For example, if a physician observes a rash about a patient’s elbow which the physician does not recognize as a symptom of the patient’s known condition, the physician can collect a video clip to illustrate the rash. While collecting the clip, the physician can dictate an audio note explaining the rash.

Prior to collecting the clip, the physician uses toggle button 325 to scroll through target server choices. Initially it will be assumed the physician simply selects “No server” using button 325 and the server indicator.

After the physician completes the examination, the physician may review the video clip via viewer 317. If the physician determines that the clip may be useful, the physician may, prior to reviewing the clip again, use button 324 to select a target server. It will be assumed the physician selects a personal archive server as the target server so that the physician can review the clipping later with the aid of medical references in her office. Then, with a target server selected, it is envisioned that any video reviewed will be earmarked for building a target server address. Thus, if a clip is 10 seconds long, the physician may only review a 4 second clip, thereby selecting the 4 second clip for delivery to the target server.

In addition, if desired, by selecting another server via button 325 and reviewing the clip again, the physician can select a second server for building yet another target address for the clip.

After her rounds, the physician accesses a terminal, transmits information packets, including or not including video, depending on what the physician selected, and edits and approves the packets. In this regard, in addition to including the typical HTML formatting information indicated above with respect to the other examples, the packets including video clips provide icons and a viewing window to enable the physician to observe and perhaps edit earmarked video clips prior to storage to a server.

In a second example of how video capable ICD 301 might operate, instead of being used in a medical facility, it will be assumed ICD 301 is used in a jet and maintenance facility for a major airline. In this example, the ICD user is a maintenance technician. It will also be assumed that many jet components include unique bar codes for identifying component parts. For example, a right wing rudder may include a bar code identifying the rudder as a right wing rudder. In addition, the code for a particular jet’s right wing rudder may indicate the specific rudder components instead of simply a right wing rudder. For example, the code may indicate “right wing rudder #8821475” so that the specific rudder and its history can be tracked.

In addition, each jet will typically be equipped with a jet specific bar code. While the bar codes may be provided on separate jet components, more typically, a maintenance technician will have a bar code binder or notebook which, for a particular jet, lists all components and the component specific bar codes. Thus, the binder would include an entry “right wing rudder #8821475” which corresponds to the specific jet. During routine maintenance check-ups, the technician is required to carry ICD 301 to collect information for a maintenance report.

During a check-up the technician would first use ICD 301 to establish an association between the jet being examined and the ICD 301. To this end, initially the technician uses ICD 301 to read the jet specifying bar code for the jet or the jet specific binder via reader 323. When the code is read, ICD 301 stores the code and identifies the time and date. At this point ICD can already formulate a good portion of a target server address for the technicians report. As the technician examines the jet, the technician can use ICD 301 to take dictation and identify other specific components via corresponding bar codes from the binder.

When the technician observes the right rudder, it will be assumed that the technician observes a small puncture in the outside skin of the rudder. To document the puncture and subsequently order maintenance services, the technician establishes an association between the right rudder and ICD 301. To this end, the technician locates the right rudder in the binder and uses reader 323 to read the code. The right rudder code is then stored by ICD 301. Next, assuming the puncture is particularly dangerous the technical immediately orders maintenance to repair or replace the rudder. In addition, the technician will want to generate a video clip for archiving so that the puncture is documented for subsequent review and for use by the person who will repair/replace the rudder.

To this end, the technician can use button 325 to scroll through the possible target servers. It is assumed ICD 301 provides a “Maintenance Server” choice. The technician selects the maintenance server as the target server and then
collects a video clip of the punctured rudder skin. The maintenance server selection causes ICD 301 to generate a target address specifying the maintenance server for the video clip. Audio information may be provided by the technician during the video clip. In addition, date, time, rudder information, jet identification and technician identification information is added to the video clip for identifying a target address and populating fields in an information packet.

[0389] After the examination, the technician accesses a terminal and downloads all information packets for observation. After examining the packet corresponding to the rudder puncture (including the clip), the technician approves the packet information and transmits the information to the maintenance server. Another maintenance technician reviews the video clip and other information provided therewith. Thereafter, the puncture is repaired or the rudder is replaced.

[0390] Where maintenance is required prior to flight, in addition to sending the clip to maintenance, the clip and associated information may also be earmarked for a clearance server, personnel associated therewith grounding all jets which require maintenance. In addition, all data collected may be achieved in an archive server regardless of whether or not the archive server is selected by the technician. In yet another example which is related to the previous example, an ICD similar to ICD 301 may be equipped with a lens 315 attached to a technician’s head piece or helmet so that everything which is viewed by a technical is captured on video. Thereafter or, during an examination, the technician could earmark certain video clips (e.g., 5-10 seconds) for delivery to specific target server addresses while the entire video is archived on an archive server.

[0391] Importantly, it should be noted that preferably content is provided within generated addresses in the present invention. For example, where several facilities share servers, a portion of each server may be earmarked for each facility and therefore all information units or documents for a specific facility should be stored in the corresponding earmarked locations. A portion of each address preferably identifies the facility from which an associated information unit originated. Thus, the address is content specific.

[0392] Similarly, for every patient at a facility, preferably, information associated with the patient, is stored at a specific location within the portion of a server earmarked for the facility. As indicated above patient information is also provided in an address. Similar address fields are provided for physician information, type of record, time, date, etc. so that virtually an entire address can specify content.

[0393] This type of content specifying address is not only intuitive but also very useful in that it makes it relatively easy to retrieve data and information units from storage. In addition, this type of addressing reduces the overall size of an information packet and information units as important content information can be stored in the address.

[0394] While a particular embodiment of the invention has been illustrated and described, it will be obvious to those skilled in the art that various changes and modifications may be made without sacrificing the advantages provided by the principle of construction disclosed herein. For example, while the invention is generally described in the context of HTML, clearly the invention is meant to be used with other conventional markup languages or with JAVA or JAVA script program codes. In addition, while the invention is described as being used with a browser, the invention could be used with any terminal which includes software which receives formatting codes and can display information as a function of such codes. Moreover, while it is preferred that full target addresses be provided by an ICD 10, clearly minimal addresses such as a coded address could be provided to a browser wherein the browser would expand the coded minimal address into a full fledged address, the advantage being that the ICD specifies where data is to be stored, not a browser or associated server.

To apprise the public of the scope of this invention I make the following claims:

1. An apparatus for use with a plurality of specifier apparatus and a network system including an input device and a plurality of network devices linked to the input device, the input device equipped to receive network device target addresses, each identifying one of the plurality of network devices,
the plurality of specifier apparatuses each representing at least one target address,
the apparatus for remotely collecting at least one target address from at least one specifier apparatus and providing the at least one target address to the input device,
the apparatus comprising:
a data collector comprised of
a. a collector for collecting a target address from at least one specifier apparatus;
b. a processor linked to the collector for receiving the target address therefrom;
c. an output device linked to the processor for transmitting the target address to the input device; and
the input device using the target address to send a message to the network device corresponding to the target address.

2. The apparatus of claim 1 wherein the specifier apparatus is a machine readable device.

3. The apparatus of claim 1 wherein the output device also sends to the input device identification information for the data collector and the input device also sends the identification information to the respective network device as part of the message.

* * * * *