Caregiver System Technical Overview

Caregiver Alliance Web Services™ is the only consumer-controlled, interoperable personal health record system (PHR) with the security of online banking.

Caregiver Alliance Web Services™ (Caregiver) are engineered consistent with health information industry standards, operated to exceed the requirements of HIPAA security and privacy rules, and designed for future alignment with the federal government's national health information network (NHIN).

The Caregiver system integrates consumer-controlled, interoperable personal health records (PHRs) for individuals with provider-controlled, interoperable electronic health records (EHRs) for health and human service providers, educators, corrections professionals, nonprofit and state agencies, state agency alliances and regional health information organizations (RHIOs). End-to-end solutions for consumers, providers, and enterprises result from a la carte combinations of ready-to-use online accounts with customized care plans and Web services.

The Caregiver PHR is distinguished by features that address the needs of long-term care consumers, providers, and family caregivers, some of which are summarized in Table 1.

Table 1. PHR System Features & Benefits
A √ indicates a unique, patent-protected feature.

	Feature	Benefit
√ Care Plan	Disorder-specific, customized coordinated care plans automate the design, implementation, and monitoring of individualized, multi-provider, treatment.	Coordination of long-term care team members prevents medical mistakes and facilitates treatment consistent with practice guidelines and evidence-based protocols.
√ Data Exchange (Interoperability)	Consumer-authorized providers have options for online, manual exchange of data with patients' PHRs and for peer-to-peer, automated exchange of data between patients' PHRs and their EHR or EMR systems.	Consumers know that doctors and emergency responders can get vital information quickly, but without violation of consumer privacy preferences.
√ File Control	Consumer-authorized users have options for uplooading, categorizing, and retrieving digital and scanned files consistent with consumer privacy preferences.	Long-term care team members may quickly share and find vital information without violation of consumer privacy preferences.
√ Privacy	All PHR data are subject to the same consumer-authorized privileges including calendar and messages.	Consumers' privacy preferences cannot be violated either inadvertently or maliciously.
√ Privileges	The consumer (or delegated PHR account administrator) authorizes and controls role-, relationship-, and content-based privileges of PHR users.	Consumers decide who views and updates what information in their PHRs and when including emergency responders.

Table 1. PHR System Features & Benefits A √ indicates a unique, patent-protected feature.		
	Feature	Benefit
Audit Trail	An audit trail automatically records all authorized users' activities and thwarted illegal penetrations attempts.	Consumers know who is doing what in their Caregiver PHRs at all times.
Availability	The Caregiver PHR is available 24/7 from any Internet-connected computer.	Authorized users need not download software or work at a particular computer.
Calendar	A networked calendar automates scheduling and reminding, synchronizing with MS Outlook.	Long-term care team members complete and document assignments.
Data Persistence	Data entered into PHRs may be archived or annotated but never deleted.	Vital consumer data cannot be destroyed either inadvertently or maliciously.
Security	The Caregiver PHR system employs data encryption and other other online banking security practices.	Consumer data are protected against intrusion.
Web Messaging	A secure Web messaging function is available to all authorized users, with the option for automated email alerts about the availability of new messages.	Consumers can communicate with their doctors in a secure manner free from the vulnerabilities of email.

Caregiver core and edge systems. The core Caregiver system includes ready-to-use, turnkey accounts and engines that permit Caregiver edge systems to fulfill specific customer requirements. Caregiver edge systems, also known as templates and modules, cannot function independently of the core system. These system building blocks are licensed for use by customers who request specific assemblies of user interfaces, features, and functions.

Caregiver system operation. The Company adopts best industry practices for system operation including the following: periodic scan of uploaded files for viruses; daily code security updates when available; minimum necessary network services and installed packages; daily log reviews; nonstandard SSH access port; regular off-site backups of application data to a secure system. The Company's servers reside in a secure hosting facility with redundant Internet connections on opposite sides of the building, fire suppression equipment, battery and diesel power back-up.

Application testing. The Company employs a test plan to verify correct functioning of the application. Future plans include automated performance testing to measure application response time.

Escrowing of software code. A copy of current source code including technical documentation and installation instructions is periodically shipped to our corporate attorney for escrow.

Turnkey User Accounts

Each person with Caregiver access privileges, or user, has a unique system-wide user-ID and self-selected password. With user-ID and password, users may log on 24/7 to the Caregiver system from any Web browser. A user's first destination after logging on is the turnkey user account. Users are required to provide ample user identification information as a condition for Caregiver system access. This information is employed to properly identify users (including users who are named clients on client accounts) and to autopopulate fields in accounts that the user accesses. From the user account home page, the user selects and enters client accounts consistent with the user's account-specific privileges. The user account stores information about past and present access privileges to all accounts.

Turnkey Client Accounts--PHRs

The Caregiver client account is a lifetime, comprehensive, personal health record (Caregiver PHR client account). The Caregiver PHR client account is the hub of the Caregiver authorization and privacy model. All client account information is treated as HIPAA-designated personal health information. All client account information is permanent (subject to archiving but not to deletion).

> Each client account has an account administrator. The account administrator establishes authorized users and manages user access privileges. The account administrator decides what information to retire from view (archive) and to restore to view.
>
> Client accounts offer three methods of privilege management: bottom-up, top-down, and combined bottom-up/top-down:
>
> - In the bottom-up method, the account administrator is the client or a client-representative (e.g., family caregiver, parent, spouse, court-appointed guardian). The bottom-up account administrator manages all privileges for client account users.
> - In the top-down method, the account administrator is the security and privacy officer (SPO) of an enterprise account (or an SPO representative). The top-down account administrator manages all privileges for client account users.
> - In the combined bottom-up/top-down method, both the client account administrator and the enterprise account SPO have privilege management capabilities.
> - Changes may be made in a client account's method of privilege management at any time.
>
> Data availability corresponds to the method of privilege management. In client accounts employing bottom-up privilege management, clients have access to all account data. In client accounts employing combined bottom-up/top-down privilege management, clients have access to all account data and enterprises have access to all account data entered by users they authorized. In client accounts employing top-down privilege management, enterprises have access to all account data.

Multiple users may have simultaneous access to a client account. The numbers of users that may access the account, at no additional charge, depend upon terms of the account subscription. Options are available for adding users to any client account.

Storage space varies depending upon terms of the client account subscription. Options are available for adding storage space to any client account at any time.

Each client account offers a full range of features. Depending upon their privileges, each user of a client account may employ features including:

- Emergency Responder Access
- Dashboard
- Account Administration
- Vital Information Logs
- Everyday Charts
- Calendar
- Messages
- File Management
- Data Export to External Storage Media
- Printing

The account administrator enters data and files into Vital Information Logs and authorizes access by emergency responders and account users. The client may carry a wallet-sized card giving emergency responders a URL, user-ID, and password for login. From the home page of the client account, emergency responders may access Vital Information Logs per account administrator authorization. The client may carry a wallet-sized CD with copies of Vital Information Logs (entries and files) per account administrator authorization. From the client account left toolbar, consistent with their privileges, users may view or update Everyday Charts, attach files to entries, and retire entries.

Turnkey Web Services

Account management. Each client account offers the designated account administrator (who may be an enterprise account security and privacy officer, SPO, or designee) features for account management and user authorization. This enables the account administrator to designate and change authorized users' roles (sets of account access privileges). A user may occupy one or more roles on a particular client account. A user may also occupy various roles in different client accounts. The enterprise account provides the SPO with functionality for assigning roles on groups of client accounts to groups of enterprise account users.

Data entry. Vital Information Logs, Everyday Charts, and Enterprise Records are the primary vehicles for entering and storing free text information and attached files in client accounts. Autopopulation from previously entered data fields reduces the need for redundant data entry. Authorized users, consistent with their privileges, may permanently update logs and charts with text entries, event date, and attached files. Users may describe log and chart entry types. Upon creation of a log or chart entry, the entry is automatically stamped with entry time and date and User-ID. By default, only the account administrator updates Vital Information Logs, keeping them current for emergency responders. Enterprise Records include records pertinent to multiple enterprises (that offer services to a particular client). Access to the records of a particular enterprise in a client account is determined by the enterprise account SPO. Enterprise account SPOs may grant privileges to users on one another's accounts to view records within a client account.

File management. Authorized users may upload electronic files of any file type into the client account. These files may then be stored in the general file repository and linked to specific vital information log or chart entries. When uploaded or linked, files may be referenced by keywords and names for ease in future searches. Users may view files in the account consistent with their privileges.

Calendar, scheduling, and accountability. Authorized users may employ calendar functions for online scheduling of events, invitation of attendees, and notification of supervisors. Users are required to specify the type of event (e.g., meeting, task), the chart category to which the event corresponds (e.g., education), the date(s) and time(s) of the scheduled event, event attendees and supervisors. Only users authorized with read privileges on that chart category are available for invitation to the event or for subsequent viewing of the event in the client account calendar. After an invitation is issued to a scheduled event, invited users receive automatic invitations by secure messages (not email), the event is included in the invited user's calendar, and the event is displayed in the invited user's upcoming-events tickler (on the user account home page).

Messaging. All accounts permit the exchange of secure messages among authorized account users without dependence upon virus-vulnerable email. Messaging may be completely internal to the Caregiver system, or may combine internal messaging and external messaging.

Priority email. A user with a provider account may specify a priority email address for alert messages. These can be configured to support rapid delivery of alert notifications to an email capable wireless device, such as a pager or mobile phone.

Customized Web Services

The Caregiver system offers various customized services that meet the business needs of nonprofit and state agencies, local agency alliances, and regional health information organizations. These include:

Care plans. Customized care plan templates automate the delivery and financing of services by multiple agencies and providers to individuals with specific needs and disorders (e.g., children with disabilities, juvenile offenders, cancer survivors). Standard data elements in the care plan are autopopulated from the client account. Previous versions of care plans are automatically preserved when new versions are created. Care plans trigger notifications, reminders, calendar entries, and supervisory alerts. Care plan data may be aggregated across clients for treatment outcome and program evaluation purposes; within and across providers and supervisors for supervisory and human resource purposes; and, within and across agencies for resource leveraging and economic analysis purposes.

Workflow engines. Customized workflow engines automate the delivery and supervision of services by one agency or a collective of partnered agencies. Workflow engines may be designed to support malpractice and professional practice guidelines, state or federal regulations, grant or contract requirements. Workflow engines yield persisting data useful in documenting adherence to multiple reporting and oversight demands.

Data exchange. Customized data exchange templates allow for one-stop data entry into familiar data-entry screens while updating multiple software databases.

Client-server installations. Customized client-server installations permit agencies with internal information technologists to host frozen versions of turnkey and customized services.