FIRST WATCH®

Helping the Helpers

FIRSTWATCH SOLUTIONS, INC. SOFTWARE LICENSE AGREEMENT

1. *Parties; Effective Date***.** This Software License Agreement ("Agreement") is between FirstWatch Solutions, Inc., 1930 Palomar Point Way., Suite 101, Carlsbad, California 92008 ("FirstWatch") and the County of El Dorado, a political subdivision of the State of California ("Client" or "Agency"). This Agreement is effective on the date last signed ("Effective Date").

2. *Purpose of Agreement.* FirstWatch is a provider of data monitoring and biosurveillance software and related services to organizations and agencies in the fields of public health and public safety. Client desires a license to use the FirstWatch software identified on Schedule A ("Software") according to the terms of this Agreement.

3. *Grant of License.* FirstWatch grants Client a license to load and execute the Software on a computer located at the Site identified on Schedule A for use by its employees and staff in connection with its syndromic surveillance system. Client may make backup and archival copies of the Software.

4. *License Term; Maintenance Services*. The term of the Software license is perpetual. However, Client shall be entitled to Software updates, upgrades, enhancements, new versions, bug fixes, other improvements to the Software and access to the FirstWatch Subscriber Site, and to technical assistance relating to the Software, for the term(s) described in Schedule A of this Software License Agreement and with payment in full for the maintenance portion of the agreement. The term of Software Maintenance and Support commences upon the date of Software Acceptance.

5. *FirstWatch Intellectual Property Rights*. The license is nontransferable and nonassignable without the prior, written permission of FirstWatch. Client may not modify, enhance, or create derivative works, decompile, disassemble, or reverse engineer the Software, or make copies other than as authorized in Section 3. All rights not licensed are reserved to FirstWatch and no rights may be implied. FirstWatch retains all intellectual property rights in the Software, and Client agrees to implement software protection measures designed to prevent unauthorized use and copying of the Software.

6. *Delivery, Installation, and Testing.* Client is responsible for acquiring all hardware, equipment, and other software; for preparing the site (including physical and electrical requirements); for properly configuring the computing environment on which the Software will reside, and for installing the Software in accordance with Schedule A and any other requirements provided by FirstWatch in writing. Client shall test the Software within ten (10) days after FirstWatch has enabled Client's access to the Software.

7. *Acceptance.* The Software is Accepted upon the earlier of when (a) Client determines that the Software performs in accordance with the criteria set forth in the Acceptance Test Plan ("ATP"), set forth in Schedule C, or (b) the Software has been installed for thirty (30) days and Client has not advised FirstWatch that the Software fails to materially conform to the ATP. If the Software does not so perform for reasons inherent in the Software (and not, for example, third party hardware, software, equipment, or system configuration), FirstWatch will promptly replace the Software with materially conforming Software. Client shall test the revised Software and, unless the parties agree otherwise, Client may either (1) Accept the Software as conforming, (2) Accept the Software AS IS, or (3) reject the Software. If Client rejects the Software, it shall delete the Software from its computing system, shall certify in writing such deletion, and FirstWatch shall refund all Software license fees paid by Client. Client shall have thirty (30) days after initial delivery to finally Accept or reject the Software. The foregoing is the sole remedy available in the event of nonconforming Software.

8. *Client Satisfaction.* FirstWatch desires that Client is fully satisfied with the Software and Services. If, within ninety (90) days after acceptance, for any reason, Client is not satisfied with the Software, Client may elect to return the Software and receive a full refund of all Software license fees paid to FirstWatch.

9. *Fees and Payments.* Client shall pay all fees according to the terms of Schedule A. Client shall pay for all travel-related expenses (*e.g.,* ground transportation, accommodations, food) incurred by FirstWatch at the request of Client and approved by Client in writing, for Software-related services such as on-site installation, training, customization, integration, support, and maintenance. Reimbursement for all travel-related expenses shall not exceed the approved rates paid under the current Client Board of Supervisor's Travel Policy in effect at the time the expenses are incurred. Such additional services will be pursuant to a separate written agreement. Client is responsible for payment of all sales and/or use taxes arising out of its use of the Software.

10. *Limited Warranties; Exclusions.* FirstWatch warrants that during the Acceptance testing period, and while Client is receiving covered Maintenance Services per section 4 of this Agreement, the Software will perform in substantial conformance with the ATP, provided that the Software has been used as specified by FirstWatch. FirstWatch will use its best efforts to correct any material nonconformance within ten (10) business days after receipt of written notice of such

nonconformance and Client's provision of any data, output, or other documentation or description of the nonconformance.

The limited software warranty applies only to Software used in accordance with the Agreement and does not apply if the Software media or Software code has been subject to accident, misuse, or modification by a party other than FirstWatch or as authorized by FirstWatch.

FirstWatch does not warrant that the functions contained in the Software will meet Client's specific needs, industry requirements, be error-free, or operate without interruption. The remedies in this Section 10 are the sole and exclusive remedies provided by FirstWatch relating to the Software.

THESE LIMITED WARRANTIES ARE IN LIEU OF, AND CLIENT HEREBY WAIVES, ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

11. *Limitation of Liability.* Neither party shall be liable for indirect, incidental, consequential, special, punitive or exemplary damages, or for lost profits or business interruption losses, in connection with the Software or this Agreement, regardless of whether it has been made aware of their possibility. Other than amounts due to a party pursuant to Sections 9 or 13, or the breach of Sections 4, 5, or 14, in no event shall either party be liable to the other, under any theory of recovery, including contract, negligence, strict liability, warranty or products liability, in an amount in excess of the amount Client paid to FirstWatch for products and services. Any claims relating to this Agreement shall be brought within two (2) years after the occurrence of the event giving rise to the cause of action.

12. Default, *Termination, and Cancellation.*

A. Termination by Default: If either party becomes aware of an event of default, that party shall give written notice of said default to the party in default that shall state the following:

1. The alleged default and the applicable Agreement provision.
2. That the party in default has ten (10) days upon receiving the notice to cure the default (Time to Cure).

If the party in default does not cure the default within ten (10) days of the Time to Cure, then such party shall be in default and the party giving notice may terminate the Agreement by issuing a Notice of Termination. The party giving notice may extend the Time to Cure at their discretion. Any extension of Time to Cure must be in writing, prepared by the party in default for signature by the party giving notice, and must specify the reason(s) for the extension and the date in which the extension of Time to Cure expires.

If Client terminates this Agreement, in whole or in part, for default:

1. Client reserves the right to procure the goods or services, or both, similar to those terminated, from other sources and FirstWatch shall be liable to Client for any excess costs for those goods or services. Client may deduct from any payment due, or that may thereafter become due to FirstWatch, the excess costs to procure from an alternate source.
2. Client shall pay FirstWatch the sum due to FirstWatch under this Agreement prior to termination, unless the cost of completion to Client exceeds the funds remaining in the Agreement. In which case the overage shall be deducted from any sum due FirstWatch under this Agreement and the balance, if any, shall be paid to FirstWatch upon demand.
3. Client may require FirstWatch to transfer title and deliver to Client any completed work under the Agreement.

The following shall be events of default under this Agreement:

1. Failure by either party to perform in a timely and satisfactory manner any or all of its obligations under this Agreement.
2. A representation or warranty made by FirstWatch in this Agreement proves to have been false or misleading in any respect.
3. FirstWatch fails to observe and perform any covenant, condition or agreement on its part to be observed or performed under this Agreement, unless Client agrees, in writing, to an extension of the time to perform before that time period expires.

B. Bankruptcy: Client may terminate this Agreement immediately in the case of bankruptcy, voluntary or involuntary, or insolvency of FirstWatch.

C. Ceasing Performance: Client may terminate this Agreement immediately in the event FirstWatch ceases to operate as a business or otherwise becomes unable to substantially perform any term or condition of this Agreement.

D. Termination or Cancellation without Cause: Client may terminate this Agreement in whole or in part, for convenience upon thirty (30) calendar days' written Notice of Termination. If such termination is effected, Client will pay for satisfactory services rendered before the effective date of termination, as set forth in the Notice of Termination provided to FirstWatch, and for any other services that Client agrees, in writing, to be necessary for contract resolution. In no event, however, shall Client be obligated to pay more than the total amount of the Agreement. Upon receipt of a Notice of Termination, FirstWatch shall promptly discontinue all services affected, as of the effective date of termination set forth in such Notice of Termination, unless the Notice directs otherwise.

13. *Indemnification.* FirstWatch agrees to defend, and hereby indemnifies, Client, from all damages, losses, fees, and expenses awarded by a court of competent jurisdiction, or reached through a settlement, arising out of Client's use of the Software or Documentation when such claim is based upon a third party claim that the Software infringes a U.S. patent, trademark, copyright or trade secret; provided that (a) Client promptly notifies FirstWatch in writing of such claim; (b) FirstWatch has sole control over the investigation, litigation and negotiation of such claim; (c) Client is current in its payments and in compliance with its obligations under this Agreement; and (d) Client reasonably cooperates, at the expense of FirstWatch, in the defense or settlement of such claim. This indemnification applies only to the Software delivered by FirstWatch and shall not apply if the Software has been modified by party other than FirstWatch, or if the Software has been combined with (or used in connection with) other products and used as a part of an infringing process or method which, but for the combination, would not infringe the intellectual property rights of such third party.

If the Software becomes, or in the opinion of FirstWatch is likely to become, the subject of such a claim, then FirstWatch may either (a) procure (at its expense) Client's right to continue using the Software, or (b) replace or modify the Software to avoid the claim of infringement. If neither of the foregoing alternatives is reasonably available to FirstWatch, then FirstWatch may terminate this license and refund to Client the license fees paid for the Software on a straight-line three (3) year depreciation basis. This agreement states the entire liability of FirstWatch with respect to third party claims of intellectual property infringement.

14. *Confidentiality.* FirstWatch and Client may have access to information that the other considers to be confidential, private, or a trade secret. This information may include, but is not limited to, patient or other data, the Software, technical know-how, technical specifications, software code, manners of conducting business and operations, strategic business plans, systems, results of testing, financial information, and third-party information ("Information"). Each party shall use the other's Information only to perform its obligations under, and for the purposes of, the Agreement. Neither party shall use the Information of the other for the benefit of a third party. Each party shall maintain the confidentiality of all Information in the same manner in which it protects its own information of like kind, but in no event shall either party take less than reasonable precautions to prevent the unauthorized disclosure or use of the Information.

Upon termination of the Agreement, or upon a party's request, each party shall return to the other all Information of the other in its possession. All provisions of the Agreement relating to confidentiality, ownership, and limitations of liability shall survive the termination of the Agreement.

15. *Ownership of Data.* The parties acknowledge and agree that all Client data ("Data"), is and shall remain the exclusive property of Client. FirstWatch acknowledges that in performing its obligations under the Agreement it may have access to Client networks and Data. FirstWatch will use and access such Data only as necessary for the purpose of providing the services and supporting the Software as agreed.

16. *HIPAA.* With respect to any protected health information ("PHI") and to the extent FirstWatch is subject to the provisions of the Health Insurance Portability and Accountability Act as a Business Associate, FirstWatch shall (a) not use or disclose PHI other than as permitted or required by any agreement between FirstWatch and Client, or as required by law, (b) use appropriate safeguards to prevent use or disclosure of the PHI, (c) report to Client any unauthorized use or disclosure of the PHI of which it becomes aware, (d) ensure that any agent or subcontractor that accesses PHI in order to assist FirstWatch in providing the Services will be bound by the provisions of this Section, (e) reasonably cooperate with Client to make its internal practices, books, and records, including policies and procedures relating to the use and disclosure of PHI available to a governmental agency in the event a governmental agency requests such information, (f) document all its disclosures of PHI and information related to such disclosures, and notify Client of such disclosures, (g) return or destroy all PHI upon termination of the Services under this Agreement. If the parties enter into a separate agreement regarding the use of protected health information, the terms of that separate agreement shall take precedence and control over the terms of this Section 16.

17. *Cooperative Purchasing.* If agreed to by Client and FirstWatch, another public body may utilize this contract. FirstWatch shall deal directly with any public body authorized to use the contract. Client, its officials and staff are not responsible for placement of orders, invoicing, payments, contractual disputes, or any other transactions between FirstWatch and any other public bodies, and in no event shall Client, its officials or staff

be responsible for any costs, damages or injury resulting to any party from use of a Client Contract. Client assumes no responsibility for any notification of the availability of the contract for use by other public bodies, but FirstWatch may conduct such notification.

18. *Contract Administrator*. The Client Officer or employee with responsibility for administering this Agreement is Michelle Patterson, MPH, Manager, Emergency Medical Services Agency, or successor.

19. *HIPAA Compliance*. As a condition of FirstWatch performing services for the Client, FirstWatch shall execute that Business Associate Agreement which is attached hereto as Schedule "B", which is incorporated herein for all intents and purposes.

20. *General*. All required communications shall be in writing and addressed to the recipient party at its address set forth in this Agreement, addressed to the person who signed the Agreement on behalf of such party, or to such address and person as may be designated by such party in writing. All communications are deemed given when hand-delivered; or if mailed, by registered mail with verification of receipt, upon date of mailing; or if by electronic mail or facsimile, when received (with verification of transmission sent promptly to the receiving party along with a hard copy of the communication).

Any part of the Agreement held to be invalid or unenforceable, shall be revised so as to make it valid and enforceable, consistent with the intent of the parties expressed in that provision. All other provisions of the Agreement will remain in full force and effect. The remedies accorded FirstWatch are cumulative and in addition to those provided by law.

The Agreement, all Schedules (A-C), and any amendments thereto constitute the entire understanding of the parties with respect to the subject matter of the Agreement and replaces all prior and contemporaneous written and oral communications, promises, or understandings. The Agreement shall be governed by the laws of the State of California and may be amended only by a writing signed on behalf of both parties. Electronic mail shall not be deemed to constitute a signed writing for purposes of this modification provision unless expressly identified as an amendment. No waiver of any right or remedy will be effective unless given in writing and signed on behalf of the party making such waiver. No purchase order or other administrative document will amend the Agreement unless signed by a representative of both parties and identified as an amendment to the Agreement, even if accepted by the receiving party without objection.

The Parties may not assign any rights or delegate any duties under the Agreement without the prior, written consent of the other Party, which will not be unreasonably withheld, and any attempt to do so without consent will be void. However, no consent shall be required in the case of a Party's transfer of all or substantially all of its business or assets by merger, asset sale, or other similar transaction. The Agreement is binding upon the parties' successors and permitted assigns.

AGREED AND ACCEPTED:

FirstWatch Solutions, Inc.

Date: 12/17/2021

By: Todd Stout
Todd Stout (Dec 17, 2021 17:53 PST)
Signature

Name: Todd Stout, President

Client Name and Address:

El Dorado County
Emergency Medical Services Agency
2900 Fairlane Court
Placerville, CA, 95667

By: ______________________________

Board of Supervisors
"County"

Dated: ____________________

Attest:
Kim Dawson
Clerk of the Board of Supervisors

By: ______________________________
Deputy Clerk

Dated: ____________________

Schedule A:

Project Services, Pricing & Payment Schedule, Contact Information & Technical Specifications

Project Services:

- Single license of FirstWatch Thin-Client (Remote Data Gathering) Software installed on Client's dedicated FirstWatch personal computer (PC)/Server

  - All data integration with Client's Data Source/System integrated via:
    - Connectivity to a data source via Open Database Connectivity (ODBC) or similar means;
    - or Text or XML ***file*** output for each incident from a Client-provided process (one [1] or more files for each incident) that provides files on the dedicated FirstWatch PC/Server;
    - or Client provided web services interface allowing FirstWatch to securely access, query, and receive necessary data via a non-dedicated internet connection. Client provided web services interface will include the ability to encrypt and decrypt data and options to query live and historical data.

  - Data Shuttle, remote connectivity and other software and processes on Client's dedicated FirstWatch PC which work together to reliably and securely transmit data to the FirstWatch Data Center, and allow for remote support, using Client-provided, always-on Internet connectivity.

  - Linking of data sources requires, at a minimum, a unique key that exists within each data source in a useable format.

- Modify centrally located FirstWatch server-based processes, software and database as necessary to receive Client's data, import into FirstWatch database, and monitor for statistically-significant increases in volume or geographic clusters of calls which meet user-defined criteria.

- Provide up to fifty (50) Client-specific user login(s) and password(s) to allow up to fifty (50) simultaneous users on the FirstWatch subscriber Internet site. (Access by additional users may be purchased, and access via FirstWatch to other, 3rd-party services or tools, may be licensed separately.)

- Provide the ability for the Client to define all system included and client purchased "trigger sets" for monitoring by FirstWatch.

- Provide the ability for the Client to define up to fifty (50) alert recipients for each trigger, via a combination of email, text messaging, fax, or compatible paging system.

- Provide a default "All Events" trigger with monitoring and alerts to demonstrate complete functionality of system.

Pricing and Payment Schedule:

Client FirstWatch Pricing				
Line #	Description	Qty.	Unit	Extended
1	Base System License* (DS1 – ImageTrend Electronic Patient Care Reporting (ePCR) – Countywide – License Transfer from Cal Tahoe Joint Powers Authority (JPA)	1	$23,656	$0
2	Annual Support & Maintenance* (DS1)	1	$5,204.32	$5,204.32
3	Data Source Integration (DS1)	1	$7,500	$7,500
4	Installation / Configuration	1	$2,500	$2,500
5	Training / Trigger Consultation / Project Management	1	$9,500	$9,500
6	System License* (DS2 – CALFIRE Northrup Grumman Computer Aided Dispatch [CAD])	1	$16,560	$16,560
7	Annual Support & Maintenance* (DS2)	1	$3,643.20	$3,643.20
8	Data Source Integration (DS2)	1	$7,500	$7,500
9	System License* (DS3 – South Lake Tahoe Fire Department Cyrun CAD & SunRidge RIMS CAD after conversion)	1	$16,560	$16,560
10	Annual Support & Maintenance* (DS3)	1	$3,643.20	$3,643.20
11	Data Source Integration (DS3) ($3,750 for Cyrun CAD and $3,750 for SunRidge RIMS CAD)	1	$7,500	$7,500
12	Standard System Triggers (Included)	20	Incl.	Incl.
13	Customized FirstWatch Reports Development (hours) for Ambulance Patient Offload Times (APOT)	10	$200	$2,000
14	Customized FirstWatch Reports Annual Support & Maintenance for APOT	10	$44	$440
15	Interactive Data Visualization Module (IDV)	1	Incl.	Incl.
16	Online Compliance Utility Module (OCU)	1	$37,500	$37,500
17	OCU Annual Support & Maintenance	1	$8,250	$8,250
18	Additional OCU Add-on Authority/Contractor	1	$5,625	$5,625
19	Additional OCU Add-on Authority/Contractor Annual Support & Maintenance	1	$1,237.50	$1,237.50
20	Additional monitored OCU Data Source	1	$9,375	$9,375
21	Additional monitored OCU Data Source Annual Support & Maintenance	1	$2,062.50	$2,062.50
22	FirstPass Module	1	$30,000	$30,000
23	FirstPass Annual Support & Maintenance	1	$6,600	$6,600
24	Additional FirstPass Add-on Agency	1	$5,000	$5,000
25	Additional FirstPass Add-on Agency Annual Support & Maintenance	1	$1,100	$1,100
26			**Total Price**	**$189,300.72**

* License and Maintenance costs are for monitoring Client's Emergency Medical Services Agency's (EMS) Calls. Assumptions are based on fifteen thousand (15,000) annual incidents, and include a 'buffer' of plus or minus (±) twenty percent (20%) of the call volume.

“Client” FirstWatch Payment Schedule	
Project Initiation Payment: Fifty percent (50%) >Invoiced for at Contract Execution	$94,650.36
FirstWatch Base System (DS1) Installation Payment: Forty percent (40%) >Invoiced for at Base System Installation	$75,720.29
FirstWatch Base System (DS1) Acceptance Payment: Ten percent (10%) >Invoiced for at Base System Acceptance (ATP)	$18,930.07

Maintenance fees beyond the Term of this Agreement (one [1] Year) will recur and reflect then-current FirstWatch maintenance and support rates unless otherwise agreed on by both parties. Annual Support Fee increase is projected (for budget purposes) at three percent (3%) per year.

Estimated Annual Support & Maintenance for Year 2	$33,146.14
Estimated Annual Support & Maintenance for Year 3	$34,140.53
Estimated Annual Support & Maintenance for Year 4	$35,164.74
Estimated Annual Support & Maintenance for Year 5	$36,219.68

FirstWatch will provide pricing for the next five (5) years ninety (90) days prior to the end of the initial term. At that time, the compensation can be incorporated through a fully executed amendment.

Switching Data Sources to a “LIVE” OCU and/or FirstPass Module(s) and/or Customized Report Developments: Timing and Financial Considerations

At least a ninety (90) day notice of a proposed data source change for the FirstWatch OCU and FirstPass Modules and Customized Reports is *highly recommended* as it will allow both parties an opportunity to better prepare to be ready. Should less notice be given, FirstWatch shall do its best to manage the required changes, but that may mean it may not be ready when needed.

*OCU Module

When Client has FirstWatch OCU enhancement module LIVE and switches to new CAD system; A Data Source Re-Configuration Fee of up to $12,000 will be required to modify and validate OCU compliance tests and automated queue-based processes as well as OCU reports against Client’s new CAD system data. This is in addition to a $7,500 new Data Source Interface fee for the base FirstWatch system (for total of $19,500), When Client has OCU live under one (1) response time compliance contract, and their response time compliance contract requirements are changed such that the OCU must be changed, there shall be a Contract Re-Configuration Fee of up to $6,000.

*FirstPass Module

When Client has FirstWatch FirstPass enhancement module LIVE and switches to new ePCR system; a FirstPass Re-Configuration Fee of up to $12,000 shall be required to modify and validate FirstPass protocol tests and automated queue-based processes and FirstPass reports against Client’s new ePCR system data. This is in addition to a $7,500 new Data Source Interface fee (for total of $19,500).

*Customized Report Development

When Client has FirstWatch Customized Reports and switches to new CAD, ePCR, Records Management System (RMS) (or other data system); a quote will be provided for the required Report Re-Configuration. This is in addition to a $7,500 fee for each new Data Source Interface required (one [1] each for new CAD, ePCR, RMS, etc.). Report Re-Configuration and data mapping, testing & validation is needed to confirm that all FirstWatch Report generation processes are functioning correctly against all new data sources.

Contact Information:

Licensor Contact Tax ID No: **05-0544884**	Todd Stout, President FirstWatch® 1930 Palomar Point Way, Suite 101 Carlsbad, California, 92008	Phone : 760-943-9123 Fax : 760-942-8329 Email : admin@firstwatch.net
Client Contact	County of El Dorado Emergency Medical Services Agency 2900 Fairlane Court Placerville, California 95667 Michelle Patterson, MPH EMS Manager	Phone : 530-919-4996 Email : michelle.patterson@edcgov.us
With a Copy to:	County of El Dorado Chief Administrative Office 330 Fair Lane Placerville, California 95667 Michele Weimer Procurement and Contracts Manager	Phone : 530-621-5670 Email : michele.weimer@edcgov.us

Technical Specifications:

FirstWatch Hardware Requirements:

Minimum (only if using existing equipment)	**Preferred** (required/minimum if new equipment)
Dedicated PC or Virtual Machine used exclusively for FirstWatch purpose	Dedicated Server or Virtual Machine used exclusively for FirstWatch purposes
Core i3 (Dual core or better)	Core i5 (Quad core or better)
4GB Random Access Memory (RAM) or better	8GB RAM or better
256 Gigabyte (GB) Disc (Partition as appropriate)	500GB Disc (Partition as appropriate.)
1 GB Ethernet Card	1 GB Ethernet Card
Any recent generation Graphic card	Any recent generation Graphic card
Keyboard/Mouse/Monitor (KVM)/Virtual Machine Access	Keyboard/Mouse/Monitor/KVM/Virtual Machine Access

FirstWatch Software Requirements:

Minimum	**Preferred**
Microsoft (MS) Windows Server 2012 or Windows 10 Professional including all the latest updates and patches loaded	Microsoft Windows Server 2016 (64bit) including all the latest updates
If the database to be monitored is MS SQL Server, SQL Server Management Studio needs to be installed. **NOTE:** For general installations, we do not need an instance of MS SQL Server installed on the server—just management studio tools.	If the database to be monitored is MS SQL Server, SQL Server Management Studio needs to be installed. **NOTE:** For general installations, we do not need an instance of MS SQL Server Database Engine installed on the server—just management studio tools.
ODBC driver or other licensed and approved connectivity to underlying database	ODBC driver or other licensed and approved connectivity to underlying database
Virus Protection Software of Client's choosing	Virus Protection Software of Client's choosing
WinZip or compatible software - Not Required if functionality included in Windows OS	WinZip or compatible software - Not Required if functionality included in Windows OS
Microsoft .NET Framework Version 4.0. (Installed with local FirstWatch Thin Client Software)	Microsoft .NET Framework Version 4.0. (Installed with local FirstWatch Thin Client Software)
Automated Time synchronization software or process of clients choosing. MS Windows OS feature is fine.	Automated Time synchronization software or process of clients choosing. MS Windows OS feature is fine.

Remote-Client Technical Specifications Continued

Connectivity, Firewall & Environment:
Always-on, high speed broadband Internet connectivity under Client specified and controlled security settings; Recommend static Internet Protocol (IP) address with hardware firewall.
Read-only Network access to database(s) being monitored **(ODBC connection)**
Outbound only access for **HTTPS (port 443) with access to *.firstwatch.net. IP Addresses for outbound whitelisting: 66.185.165.130/28, 66.185.165.131, 66.185.165.132, 66.185.165.144/29, 66.185.165.194/28, 66.185.165.195, 216.145.126.192/27, 38.70.192.112/28, 38.142.170.144/29, 38.104.122.120/29, 38.96.10.224/28.**
For agencies using FirstWatch provided Cisco WebEx Remote Access Agent service for installation and support, it may be necessary to create an exception list for WebEx sites on the firewall or proxy to properly use WebEx services. In most cases, the IP Range that can be used to add an exception for the firewall or proxy is 64.68.96.0 - 64.68.127.255 and ports 80, 443 and 1280.
Local (not domain) server **administrator** account with access to specifications above.
To maximize system availability FirstWatch recommends remote-client hardware be located with other critical systems and when possible, include UPS, back-up generator, monitored data circuits) and heating, ventilation, and air conditioning (HVAC) controlled secure environment.

Support:

Minimum
Allow FirstWatch access to the dedicated machine via WebEx Remote Access client services (or authorized substitute, including Virtual Private Network [VPN]). WebEx Remote Access client software provided with FirstWatch under maintenance and service agreement. If VPN or other connection requires additional hardware or software on client or support side, it will be the responsibility of the Client to supply it. FirstWatch understands that some agencies require attended remote access sessions and are fine with this approach when required.

Disclaimer: Although FirstWatch requires a dedicated machine for our applications, some clients have requested running the FirstWatch applications on a server that is shared with other applications. We have successfully deployed in a combination of these configurations and are willing to attempt an install in this environment if the Client understands that there is risk involved. The risk is that if another process or application on the same machine renders the machine unresponsive, it could potentially stop the processing of the FirstWatch applications. Conversely, the FirstWatch applications may affect the other applications. Therefore, if the Client decides to move forward in this manner and results in ongoing issues with FirstWatch applications, we will respectfully request that our system be transferred to a dedicated machine for the purpose of running the FirstWatch applications. FirstWatch staff will be happy to assist the Client with reconfiguring the FirstWatch system on a new machine.

Schedule B:

FirstWatch Solutions, Inc.
HIPAA Business Associate Agreement
Between FirstWatch Solutions, Inc. (FirstWatch) and
El Dorado County EMS Agency (Client)

This Business Associate Agreement is made part of the base contract ("Underlying Agreement") to which it is attached, as of the date of commencement of the term of the Underlying Agreement (the "Effective Date").

RECITALS

WHEREAS, Client and FirstWatch (here in after referred to as Business Associate ("BA") entered into the Underlying Agreement pursuant to which BA provides services to Client, and in conjunction with the provision of such services, certain Protected Health Information ("PHI") and Electronic Protected Health Information ("EPHI") may be disclosed to BA for the purposes of carrying out its obligations under the Underlying Agreement; and

WHEREAS, the Client and BA intend to protect the privacy and provide for the security of PHI and EPHI disclosed to BA pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191 of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH" Act), and regulation promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws as may be amended from time to time; and

WHEREAS, Client is a Covered Entity, as defined in the Privacy Rule and Security Rule, including but not limited to 45 CFR Section 160.103 ; and

WHEREAS, BA, when a recipient of PHI from Client, is a Business Associate as defined in the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to 42 USC Section 17938 and 45 CFR Section 160.103; and

WHEREAS, "Individual" shall have the same meaning as the term" individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.202(g);

WHEREAS, "Breach" shall have the meaning given to such term under the HITECH Act under 42 USC Section 17921; and

WHEREAS, "Unsecured PHI" shall have the meaning to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to 42 USC Section 17932(h).

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1. Definitions. Unless otherwise provided in this Business Associate Agreement, capitalized terms shall have the same meanings as set forth in the Privacy Rule, as may be amended from time to time.

2. Scope of Use and Disclosure by BA of Client Disclosed PHI

A. BA shall not disclose PHI except for the purposes of performing BA's obligations under the Underlying Agreement. Further, BA shall not use PHI in any manner that would constitute a violation of the minimum necessary policies and procedures of the Client, Privacy Rule, Security Rule, or the HITECH Act.

B. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or authorized by this Business Associate Agreement or required by law, BA may:

(1) use the PHI in its possession for its proper management and administration and to fulfill any legal obligations.

(2) disclose the PHI in its possession to a third party for the purpose of BA's proper management and administration or to fulfill any legal responsibilities of BA, or as required by law

(3) disclose PHI as necessary for BA's operations only if:

(a) prior to making a disclosure to a third party, BA will obtain written assurances from such third party including:

(i) to hold such PHI in confidence and use or further disclose it only for the purpose of which BA disclosed it to the third party, or as required by law; and,

(ii) the third party will immediately notify BA of any breaches of confidentiality of PHI to extent it has obtained knowledge of such breach.

(4) aggregate the PHI and/or aggregate the PHI with that of other data for the purpose of providing Client with data analyses related to the Underlying Agreement, or any other purpose, financial or otherwise, as requested by Client.

(5) not disclose PHI disclosed to BA by Client not authorized by the Underlying Agreement or this Business Associate Agreement without patient authorization or de-identification of the PHI as authorized in writing by Client.

(6) de-identify any and all PHI of Client received by BA under this Business Associate Agreement provided that the de-identification conforms to the requirements of the Privacy Rule, 45 CFR and does not preclude timely payment and/or claims processing and receipt.

C. BA agrees that it will neither use nor disclose PHI it receives from Client, or from another business associate of Client, except as permitted or required by this Business Associate Agreement, or as required by law, or as otherwise permitted by law.

3. <u>Obligations of BA</u>. In connection with its use of PHI disclosed by Client to BA, BA agrees to:

A. Implement appropriate administrative, technical, and physical safeguards as are necessary to prevent use or disclosure of PHI other than as permitted by the Agreement that reasonably and appropriately protects the confidentiality, integrity, and availability of the PHI in accordance with 45 CFR 164.308,164.310,164.312, and 164.504(e)(2). BA shall comply with the policies and procedures and documentation requirements of the HIPAA Security Rule.

B. Report to Client within 24 hours of any suspected or actual breach of security, intrusion, or unauthorized use or disclosure of PHI of which BA becomes aware and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. BA shall take prompt corrective action to cure any such deficiencies and any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

C. Report to Client in writing of any access, use or disclosure of PHI not permitted by the Underlying Agreement and this Business Associate Agreement, and any Breach of Unsecured PHI of which it becomes aware without unreasonable delay and in no case later than five (5) days. To the extent the Breach is solely a result of BA's failure to implement reasonable and appropriate safeguards as required by law, and not due in whole or part to the acts or omissions of the Client, BA may be required to reimburse the Client for notifications required under 45 CFR 164.404 and CFR 164.406.

D. BA shall not use or disclose PHI for fundraising or marketing purposes. BA shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates. BA shall not directly or indirectly receive remuneration in exchange of PHI, except with the prior written consent of the Client and as permitted by the HITECH Act, 42 USC Section 17935(d)(2); however, this prohibition shall not affect payment by Client to BA for services provided pursuant to the Agreement.

4. <u>PHI Access, Amendment and Disclosure Accounting</u>. BA agrees to:

A. Provide access, at the request of Client, within five (5) days, to PHI in a Designated Record Set, to the Client, or to an Individual as directed by the

Client. If BA maintains an Electronic Health Record, BA shall provide such information in electronic format to enable Client to fulfill its obligations under the HITECH Act, including, but not limited to, 42 USC Section 17935(e).

B. Within ten (10) days of receipt of a request from Client, incorporate any amendments or corrections to the PHI in accordance with the Privacy Rule in the event that the PHI in BA's possession constitutes a Designated Record Set.

C. To assist the Client in meeting its disclosure accounting under HIPAA:

(1) BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. However, accounting of disclosure from Electronic Health Record for treatment, payment, or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that BA maintains an electronic health record and is subject to this requirement. At the minimum, the information collected shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if know, the address of the entity or person; (iii) a brief description of PHI disclosed and; (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.

(2) Within in 30 days of notice by the Client, BA agrees to provide to Client information collected in accordance with this section to permit the Client to respond to a request by an Individual for an accounting of disclosures of PHI.

D. Make available to the Client, or to the Secretary of Health and Human Services (the "Secretary") , BA's internal practices, books and records relating to the use of and disclosure of PHI for purposes of determining BA's compliance with the Privacy Rule, subject to any applicable legal restrictions. BA shall provide Client a copy of any PHI that BA provides to the Secretary concurrently with providing such information to the Secretary.

5. <u>Obligations of Client</u>.

A. Client agrees that it will promptly notify BA in writing of any restrictions on the use and disclosure of PHI agreed to by Client that may affect BA's ability to perform its obligations under the Underlying Agreement, or this Business Associate Agreement.

B. Client agrees that it will promptly notify BA in writing of any changes in, or revocation of, permission by any Individual to use or disclose PHI, if such changes or revocation may affect BA's ability to perform its obligations under the Underlying Agreement, or this Business Associate Agreement.

C. Client agrees that it will promptly notify BA in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect BA's use of disclosure of PHI.

D. Client shall not request BA to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Client, except as may be expressly permitted by the Privacy Rule.

E. Client will obtain any authorizations necessary for the use or disclosure of PHI, so that BA can perform its obligations under this Business Associate Agreement and/or the Underlying Agreement.

6. Term and Termination.

A. Term. This Business Associate Agreement shall commence upon the Effective Date and terminate upon the termination of the Underlying Agreement, as provided therein when all PHI provided by the Client to BA, or created or received by BA on behalf of the Client, is destroyed or returned to the Client, or, or if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

B. Termination for Cause. Upon the Client's knowledge of a material breach by the BA, the Client shall either:

(1) Provide an opportunity for the BA to cure the breach or end the violation and terminate this Agreement if the BA does not cure the breach or end the violation within the time specified by the Client.

(2) Immediately terminate this Agreement if the BA has breached a material term of this Agreement and cure is not possible; or

(3) If neither termination nor cures are feasible, the Client shall report the violation to the Secretary.

C. Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, the BA shall, at the option of Client, return or destroy all PHI that BA or its agents or

subcontractors still maintain in any form, and shall retain no copies of such PHI.

(2) In the event that the Client determines that returning or destroying the PHI is infeasible, BA shall provide to the Client notification of the conditions that make return or destruction infeasible, and . BA shall extend the protections of this Agreement to such PHI to those purposes that make the return or destruction infeasible, for so long as the BA maintains such PHI. If Client elects destruction of the PHI, BA shall certify in writing to Client that such PHI has been destroyed.

7. Indemnity

A. BA shall indemnify and hold harmless all Agencies, Districts, Special Districts and Departments of the Client, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives (collectively "Client") from any liability whatsoever, based or asserted upon any services of BA, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to BA's performance under this Business Associate Agreement, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature whatsoever including fines, penalties or any other costs and resulting from any reason whatsoever to the extent arising from the performance of BA, its officers, agents, employees, subcontractors, agents or representatives under this Business Associate Agreement. BA shall defend, at its sole expense, all costs and fees including but not limited to attorney fees, cost of investigation, defense and settlements or awards against the Client in any claim or action based upon such alleged acts or omissions.

B. With respect to any action or claim subject to indemnification herein by BA, BA shall, at its sole cost, have the right to use counsel of its choice, subject to the approval of Client, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of Client; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes BA's indemnification of Client as set forth herein. BA's obligation to defend, indemnify and hold harmless Client shall be subject to Client having given BA written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at BA's expense, for the defense or settlement thereof. BA's obligation hereunder shall be satisfied when BA has provided to Client the appropriate form of dismissal relieving Client from any liability for the action or claim involved.

C. The specified insurance limits required in the Underlying Agreement of this Business Associate Agreement shall in no way limit or circumscribe BA's obligations to indemnify and hold harmless the Client here in from third party claims arising from the issues of this Business Associate Agreement.

D. In the event there is conflict between this clause and California Civil Code Section 2782, this clause shall be interpreted to comply with Civil Code Section 2782. Such interpretation shall not relieve the BA from indemnifying the Client to the fullest extent allowed by law.

E. In the event there is a conflict between this indemnification clause and an indemnification clause contained in the Underlying Agreement of this Business Associate Agreement, this indemnification shall only apply to the subject issues included within this Business Associate Agreement.

8. Amendment
The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Client to comply with the Privacy Rule, 45 CFR, and HIPAA generally.

9. Survival
The respective rights and obligations of this Business Associate Agreement shall survive the termination or expiration of this Business Associate Agreement.

10 Regulatory References
A reference in this Business Associate Agreement to a section in the Privacy Rule means the section as in effect or as amended.

11. Conflicts
Any ambiguity in this Business Associate Agreement and the Underlying Agreement shall be resolved to permit Client to comply with the Privacy Rule, 45 CFR, and HIPAA generally.

FirstWatch Solutions, Inc.

Date: 12/17/2021

By: Todd Stout
Todd Stout (Dec 17, 2021 17:53 PST)
Signature

Name: Todd Stout, President

Schedule C:

Acceptance Test Plan

Introduction

The FirstWatch Acceptance Test Plan (ATP) is designed to confirm with you, our Client, that FirstWatch data integration has been completed. It is also the tool by which you will be guided through the verification process of FirstWatch Base System Acceptance. Some features and functions may vary depending on data system and type. Each commonly used functionality of the product is provided an expected result for each "test" executed. These tests assume that the data made available to FirstWatch contains the information necessary to provide the functionality to test. An example would be if the underlying data available to FirstWatch does NOT contain patient destination for an ambulance call, then FirstWatch cannot make it available for the user to view or test.

No.	Test	Expected Result	Pass = Y
			Fail = N
				Comment

1	Navigate to the FirstWatch Subscriber Site subscriber.firstwatch.net	FirstWatch Subscriber Site displays	***Yes / No***	
2	Enter a Username and Password provided to you by FirstWatch.	Successfully log into Status Page showing a quick-view of one or more triggers	***Yes / No***	
3	Launch your All Calls Trigger	New window opens showing the Event List summary page	***Yes / No***	
4	Click a hyperlink field from one of the events in the line listing.	Page displays a drill-down of data related to incident/event selected.	***Yes / No***	
5	Click the View Alert Config link from the top right of the page.	Separate windows displays criteria for which this trigger will alert, or "This trigger is currently not configured for any alerts."	***Yes / No***	
6	Set Refresh Rate to 1 minute.	Page will reload every 1 minute. Prior to reloading a green "Reloading" bar will appear near the top left section of the page. Reset Refresh Rate to 20 minutes after page reloads so reloads to not interfere with ATP.	***Yes / No***	
7	Click the Graphs link from the top of the page	The GraphIt Summary page will display	***Yes / No***	
8	Check the Hide Min/Max Events box above the Actual Events Graph.	Shaded area (if present) along Actual Events line will disappear.	***Yes / No***	
9	Check the Hide Hourly Events box above the Actual Events Graph.	Green bars along bottom axis will disappear	***Yes / No***	
10	Click the Maps link from the top of the page. The Map link is only present for data sets that include geo-data	Click on the filter icon and select a sub-category in the Group By dropdown. Click an incident on the map and click the Incident Detail hyperlink to launch the incident drilldown.	***Yes / No***	
11	Click the Layers icon and click the Top 10 Problems category	A multi-colored list of the Top 10 Problems will appear	***Yes / No***	
12	Click the Destination link from the top of the page. (Only present for data sets which include patient transport destination data)	Page displays a line listing of events separated by transport destination.	***Yes / No***	

13	Click the Analysis Tool link from the top of the page.	Page displays interactive tool for retrospective analysis.	***Yes / No***	
14	Specify a Start Date/Time and Stop Data/Time of the last 7 to 10 days. (Default date range will include the last 7 days). Click Event List link.	After calculations are complete, trigger will display line listing of all events for date/time range selected.	***Yes / No***	
15	Click GraphIt link	Graphit summary for date/time range selected will display	***Yes / No***	
16	Click Maps link	Page displays MapShot of all activity for date/time range selected.	***Yes / No***	
17	Click the Go-Back to real-time link.	Page returns to Event list view.	***Yes / No***	
18	Press the Log Out button on the top right corner of this trigger.	User will be logged out and redirected to FirstWatch Subscriber site.		

Acceptance: *Test Plan Passed Successfully, Test Plan Conditionally Accepted or Test Plan Did Not Pass*

Notes:

If Conditional or Rejected please specify the reason(s) in detail

Name:

Title:

Agency:

Signature:

Date:

When completed, please email this form to admin@firstwatch.net

FIRST WATCH

Every Record. In Real Time. Automatically.

Exhibit A

FirstWatch
Remote Client Installation Guide

Section1: Quick-Start Guide
Section2: Technical Overview
Section3: Re-Installing FirstWatch Service on a new machine (Existing Clients)

This **Quick-Start Checklist** and **Technical Specifications** will walk you through the steps necessary to prepare your site for FirstWatch Installation/Integration.

Typically, IT Time to complete the Quick-Start Checklist is between is between 1 to 4 hours. Once you have completed these steps, please contact FirstWatch to schedule the installation.

At any time during the installation process if you have any questions, please do not hesitate to contact FirstWatch Integration Team directly with any questions/comments.

Email: Integrations@firstwatch.net

Telephone: 760-658-9899 / 760-658-9844

FirstWatch Solutions
1930 Palomar Point Way #101
Carlsbad, CA 92008

Every Record. In Real Time. Automatically.

Section 1: Quick Start Checklist

	1. Set up a dedicated FirstWatch PC/Server that meets the Technical Specifications on page 3. (See Hardware configuration example on Page 10) 2. Create a local machine account for FirstWatch with local **administrative privileges**, or an account with the ability to start & stop Services. (Why a local admin account? See FAQ on Page 7) 3. Configure & Test always on Internet Connection > 40 Mbps. **FirstWatch only requires outbound https, which is typically done over port 443.**
	4. If FirstWatch is connecting directly to data source(s) via ODBC, install **SQL Server Management Studio Tools** –for MS SQL Server database. Install native query tools if the database is other than MS SQL Server. (How/Why is SSMS used? See FAQ on Page 7)
	5. Install your agency's preferred **Anti-virus/Anti-Spyware** or protective software. (Read more about client responsibilities on page 6)
Windows Update	6. Ensure Operating System, Applications and Anti-Virus software is patched and updated to your agency's Specifications. (**Windows Update, Security Patches, Office Update, Virus Definitions,** etc.)
ODBC	7. If FirstWatch is connecting directly to **data source(s) via ODBC, create a read-only database** account and provide the following info: a. User ID, Password, Server Name/IP Address and Database Name **Important Note: Please do not send the credentials to FirstWatch in plain text over email. Call FirstWatch with the credentials.**
	8. If FirstWatch is receiving data through a **push process**, please provide the following information: a. Data Export Folder UNC path b. File Type (.log, .exp, txt, etc.,) c. Ensure FirstWatch machine account has adequate permission to copy/write/delete data from the data export folder
RemoteAccess	9. Configure **remote access** approach that will allow FirstWatch to remotely perform the installation and integration process. (See Tech Specs and page 6 for more info)
	10. https://*.firstwatch.net to your firewall's trusted sites. 11. **Whitelist** the following FirstWatch Email suffix on your mail server. *@firstwatch.net (may be completed after installation)

Every Record. In Real Time. Automatically.

Section 2:

Technical Specifications

FirstWatch Remote-Client (Secure Data Broker) Technical Specifications

FirstWatch Hardware Requirements:

Minimum (only if using existing equipment)	**Preferred** (required/minimum if new equipment)
Dedicated PC or Virtual Machine used exclusively for FirstWatch purpose	Dedicated Server or Virtual Machine used exclusively for FirstWatch purposes
Core i3 (Dual core or better)	Core i5 (Quad core or better)
4GB RAM or better	8GB RAM or better
256 GB Disc (Partition as appropriate)	500GB Disc (Partition as appropriate.)
1 GB Ethernet Card	1 GB Ethernet Card
Any recent generation Graphic card	Any recent generation Graphic card
Keyboard/Mouse/Monitor/KVM/Virtual Machine Access	Keyboard/Mouse/Monitor/KVM/Virtual Machine Access

FirstWatch Software Requirements:

Minimum	**Preferred**
Microsoft Windows Server 2012 or Windows 10 Professional including all the latest updates and patches loaded	Microsoft Windows Server 2016 (64bit) including all the latest updates
If the database to be monitored is MS SQL Server, SQL Server Management Studio needs to be installed. **NOTE:** For general installations, we do not need an instance of MS SQL Server installed on the server—just management studio tools.	If the database to be monitored is MS SQL Server, SQL Server Management Studio needs to be installed. **NOTE:** For general installations, we do not need an instance of MS SQL Server Database Engine installed on the server—just management studio tools.
ODBC driver or other licensed and approved connectivity to underlying database	ODBC driver or other licensed and approved connectivity to underlying database
Virus Protection Software of customer's choosing	Virus Protection Software of customer's choosing
WinZip or compatible software - Not Required if functionality included in Windows OS	WinZip or compatible software - Not Required if functionality included in Windows OS
Microsoft .NET Framework Version 4.0. (installed with local FirstWatch Thin Client Software)	Microsoft .NET Framework Version 4.0. (installed with local FirstWatch Thin Client Software)

Automated Time synchronization software or process of clients choosing. MS Windows OS feature is fine.	Automated Time synchronization software or process of clients choosing. MS Windows OS feature is fine.

Remote-Client Technical Specifications Continued

Connectivity, Firewall & Environment:
Always-on, high speed broadband Internet connectivity under customer specified and controlled security settings; Recommend static IP address with hardware firewall.
Read-only Network access to database(s) being monitored **(ODBC connection)**
Outbound only access for **HTTPS (port 443) with access to *.firstwatch.net. IP Addresses for outbound whitelisting: 66.185.165.130/28, 66.185.165.131, 66.185.165.132, 66.185.165.144/29, 66.185.165.194/28, 66.185.165.195, 216.145.126.192/27, 38.70.192.112/28, 38.142.170.144/29, 38.104.122.120/29, 38.96.10.224/28.**
For agencies using FirstWatch provided Cisco WebEx Remote Access Agent service for installation and support, it may be necessary to create an exception list for WebEx sites on the firewall or proxy to properly use WebEx services. In most cases, the IP Range that can be used to add an exception for the firewall or proxy is 64.68.96.0 - 64.68.127.255 and ports 80, 443 and 1280.
Local (not domain) server **administrator** account with access to specifications above.
To maximize system availability FirstWatch recommends remote-client hardware be located with other critical systems and when possible include UPS, back-up generator, monitored data circuits) and HVAC controlled secure environment.

Support:

Minimum
Allow FirstWatch access to the dedicated machine via WebEx Remote Access client services (or authorized substitute, including VPN). WebEx Remote Access client software provided with FirstWatch under maintenance and service agreement. If VPN or other connection requires additional hardware or software on client or support side, it will be the responsibility of the customer to supply it. FirstWatch understands that some agencies require attended remote access sessions and are fine with this approach when required.

Disclaimer: Although FirstWatch requires a dedicated machine for our applications, some clients have requested running the FirstWatch applications on a server that is shared with other applications. We have successfully deployed in a combination of these configurations and are willing to attempt an install in this environment if the client understands that there is risk involved. The risk is that if another process or application on the same machine renders the machine unresponsive, it could potentially stop the processing of the FirstWatch applications. Conversely, the FirstWatch applications may affect the other applications. Therefore, if the client decides to move forward in this manner and results in ongoing issues with FirstWatch applications, we will respectfully request that our system be transferred to a dedicated machine for the purpose of running the FirstWatch applications. FirstWatch staff will be happy to assist the client with reconfiguring the FirstWatch system on a new machine.

Rapid Deployment - Easy to Maintain

FirstWatch System was designed to be easily and quickly deployed. The science of syndromic surveillance is evolving and to be successful FirstWatch needs to evolve with it, so we have designed our system to do just that. Client-side technology needs are minimal, and include a standard Windows desktop PC, Internet connectivity and access to the underlying data. Additional needs such as anti-virus software and firewalls are already part of most client's networks so in most cases the software, hardware, and configuration costs are well under $1,000. This centralized server design allows FirstWatch to deploy new analysis tools and add new features and functionality quickly without requiring our clients to purchase new hardware or install software upgrades and patches just to keep up. With our web-based architecture we can deploy added functionality with very limited impact on the client's individual technology. In many cases the **IT Staff time commitment is typically 1 to 4 hours**.

Data Source Connectivity

The FirstWatch System uses a variety of approaches to connect to each particular data source. The most common method is to use **O**pen **D**ata**b**ase **C**onnectivity or **ODBC**. The ODBC interface was developed in 1992 and has become the standard methodology for interoperability between data sources. The ODBC approach allows FirstWatch to run low-impact queries against a client's data sources and capture the key data elements needed for analysis. The FirstWatch System is not database specific, meaning it interfaces with a variety of different systems and may already interface with yours. By interfacing directly to client's data source, FirstWatch can capture events as soon as they are entered and doesn't require any secondary data entry or changes to existing internal practices. If you plan on using a method other than ODBC, you will be working on your custom solution directly with the FirstWatch Team.

Included Support and Maintenance Services include:

24/7 Urgent/Critical Technical Support
Weekday Business Hour Support for Routine Matters
Automated Real-Time System Health Monitoring
FirstWatch Software Updates and Patches
FirstWatch Selected Software and System Enhancements
Guidance/Support in Configuration and Trigger Development

Supporting the FirstWatch PC/Server

FirstWatch is designed to function with little on-site support outside of normal system maintenance. The FirstWatch system includes a few self-healing processes and tools that alert FirstWatch Technical Support if there is a problem.

FirstWatch Software Upgrades & Patches

Most FirstWatch software upgrades and patches can be accomplished remotely and do not require any action by the client and generally do not involve any downtime.

Client's Support Responsibilities
The client is responsible to ensure that all Microsoft Windows updates, security patches and service packs are installed, as well as maintaining the anti-virus software and maintaining the firewall.

Remote Connectivity
For installation and support of your FirstWatch System we require remote connectivity. Each agency has different approaches to remote connectivity, therefore, FirstWatch will work with your agency to find the right fit. FirstWatch also recognizes the possibility of an agency having a requirement for attended access and is fine with that approach.

Cisco WebEx Remote Access Client
Our preferred method for remote connectivity is the Cisco WebEx Remote Access, which provides a secure connection to the FirstWatch PC/Server. FirstWatch will include this tool at no additional cost to the client.

Other Remote Connectivity Methods
We also routinely connect to client sites using some form of VPN. If your agency prefers using a different method, please work with the FirstWatch Team to discuss configuration.

Additional Software Requirements:

In addition to the **Windows OS**, several readily available programs should be installed and maintained by the client:

SQL Server Management Studio Tools or native query tool
These tools are used for data exploration and troubleshooting.
Antivirus Software: Selected, supported and maintained by the client.
ODBC Driver: The driver allows FirstWatch to connect to the underlying database, if not included with database or OS. FirstWatch also accepts text, XML or other "pushed" files for legacy systems without direct database access.

Every Record. In Real Time. Automatically.

Frequently Asked Questions

How long will this software installation take?

Once you have completed the FirstWatch Quick- Start Checklist you can schedule your installation. For a previously integrated data source, a new installation will take FirstWatch about 2 – 4 hours. New data sources will take longer, typically between 4 to 8 weeks. However, installations can typically be accomplished without local IT assistance.

What impact will FirstWatch have on our IT Staff?

After system installation the client is only responsible for normal maintenance of the PC/server to include operating system & anti-virus updates and other normal activities specific to your organization. Occasional routine issues may arise, but it is rare.

What is the best configuration for my FirstWatch hardware?

There are several different configurations that will work, and each client's internal structure and policies should guide this choice. The FirstWatch Operations Team can help you decide which one works best for your environment. For additional security, consider configuring your firewall to only allow outbound communications on the required ports between the FirstWatch Data Center. Please review the sample configuration diagrams on page 9.

Why does FirstWatch need 24/7 Remote Access?

FirstWatch uses remote access to support your system in the event of a technical problem and during installation and configuration. The FirstWatch system includes several monitoring systems that alert the on-call technician if any problems occur. The remote access allows the on-call technician to troubleshoot and address issues quickly.

Does the FirstWatch PC/Server really need to be dedicated for the FirstWatch System?

Yes, FirstWatch is designed to function as a stand-alone service. Running additional programs may have undesired effects on your FirstWatch System. Additionally, FirstWatch runs as a service which means the First-Watch PC/Server can stay at a login prompt for additional on-site security.

What happens if our Internet connection goes down?

Should your Internet connection go down, the remote-client will continue to process files and store data until the connection is re-established. Once the connection is restored, FirstWatch will automatically begin processing records.

Frequently Asked Questions (Continued):

Why does FirstWatch need a local administrator account?

The remote-client is configured to run as a Service, allowing the FirstWatch PC/server to be at a Windows Login Prompt. Not only does this add additional security to your network, but it also ensures the FirstWatch application will restart automatically without user interaction should the FirstWatch PC/Server need to be rebooted.

Why is Microsoft Access™ or SQL Server Management Studio part of the installation requirements?

MS Access or SQL Management Studio Tools aren't part of the FirstWatch application, but may be used during installation and maintenance of the system as a data exploration tool.

Can I change any of my current trigger subscriptions monitor something else?

FirstWatch support and maintenance provides for a total of up to (2) two trigger reconfigurations per year. If the trigger reconfiguration exceeds this pre-allocated amount an additional cost will be imposed at the current trigger rate.

Data Security Overview

The FirstWatch internal and external data transmission routine uses a multi- stage, dual level encryption and authentication process. These processes not only doubly encrypt data, but will not allow encrypted data to be transmitted to unauthorized servers.

Data Preparation

Internally behind the client firewall, Data is compressed to decrease network bandwidth usage and improve efficiency.

Initial encryption

Data is encrypted using triple DES (TDEA/TDES) 168-bit variable key-size block cipher encryption.

FirstWatch Network Authentication

FirstWatch's upload process establishes a secure connection with the FirstWatch data center and authenticates using a key-level authentication.

2048-Bit TLS/SSL Data Encryption and Authentication Process

Already encrypted data connection is authenticated, and then transmitted via Transport Layer Security (TLS) 2048-bit encryption

SSL Authentication: Client's message to Server is encrypted with Client's private key and with Server's public key. Server decrypts the message using Server's private key and Client's public key. This way, Server can be sure that Client is who authorized to send data as no one else could create a message encrypted with his private key. SSL achieves this with the use of certificates. A certificate is issued by a third party, usually a certificate issuing authority and including the public key of the certified party as well as information that can be used to check the validity of the certificate.

SSL Integrity: SSL guarantees integrity by using a MAC (Message Authentication Code) with the necessary hash table functions. On generation of a message the MAC is obtained by applying the hash table functions and it is encoded into the message. After the message has been received its validity can then be checked by comparing the MAC with the result obtained by reversing the hash functions. This prevents messages that have been altered by a third party from slipping through unnoticed.

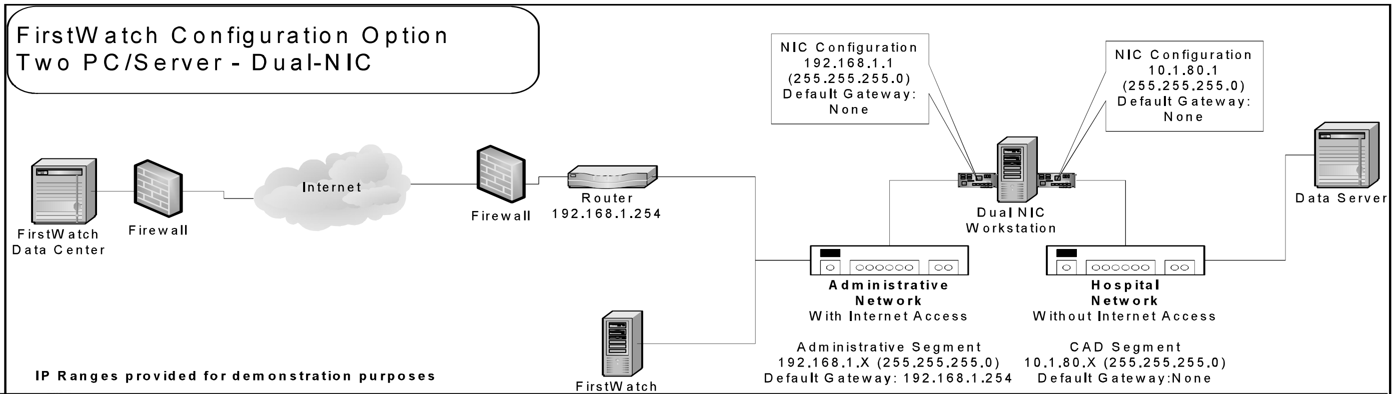
Data consumption and at rest encryption

After the data is received at the FirstWatch Data Center, the data is consumed by secure MS SQL Servers where the data is stored using Transparent Data Encryption (TDE) e.g. Data Encryption at rest. TDE per-forms real-time I/O encryption and decryption of the data and log files. The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. The DEK is a symmetric key secured by using a certificate stored in the master database of the server or an asymmetric key protected by an EKM module. TDE protects data "at rest", meaning the data and log files. It pro-vides the ability to comply with many laws, regulations, and guidelines established in various industries. This enables software developers to encrypt data by using AES and 3DES encryption algorithms without changing existing applications. FirstWatch maintains an Encryption Key Management Policy (Policy 19)

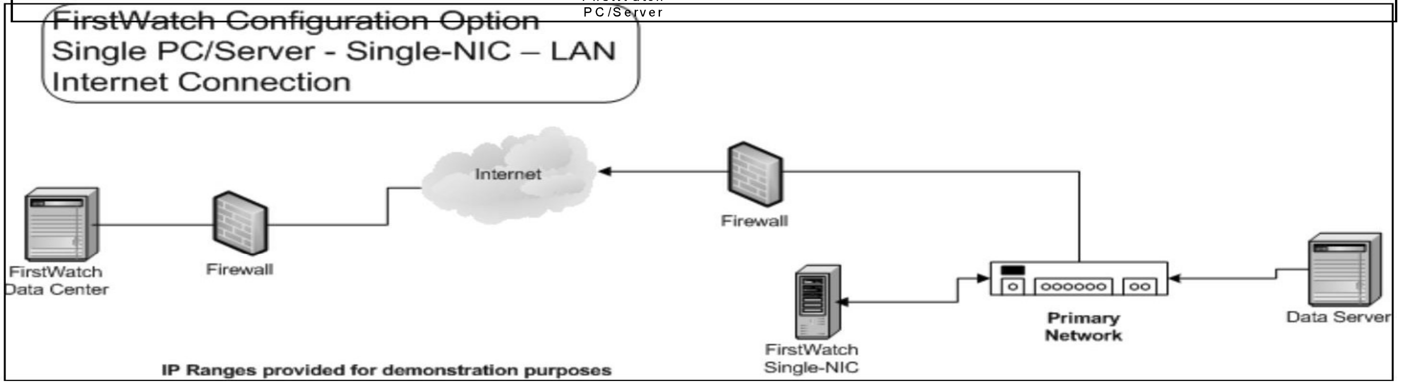
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15

Hardware Configuration Examples

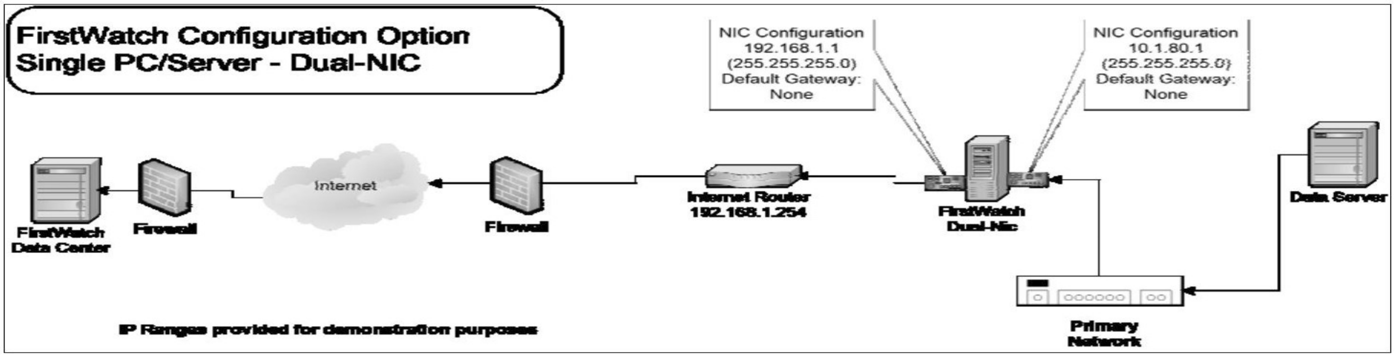
There are several approaches for configuring FirstWatch to work within a client network. Each client’s network and needs are different and the diagrams below only offer three possible suggestion and should not be considered as the only options. In all three diagrams below, FirstWatch queries data sources and shuttles encrypted data through an encrypted SSL circuit. To learn more about FirstWatch Data Security Methods, please refer to the ***Data Encryption and Authentication Overview***


FirstWatch Configuration Option
Two PC/Server - Dual-NIC

IP Ranges provided for demonstration purposes


FirstWatch Configuration Option
Single PC/Server - Single-NIC – LAN
Internet Connection

IP Ranges provided for demonstration purposes


FirstWatch Configuration Option
Single PC/Server - Dual-NIC

IP Ranges provided for demonstration purposes

Section 3:
Re-installing FirstWatch Software on a New Machine

When the time comes to refresh your hardware as it reaches end of life support terms, you may need to have the FirstWatch applications installed on a new machine. Please contact the FirstWatch Operations and Support center well in advance for planning and scheduling purposes and we'll be happy to assist you with this transition. The process of re-installing the FirstWatch application is relatively straightforward. Once you have completed the initial preparation steps, a FirstWatch Support team member will be required to complete the re-installation of your system. The following steps provide a guideline of the preparation steps required be-fore FirstWatch can be re-installed on your new machine.

Note: Since there is already an existing Read-Only database account, you do not need to create a new one at the server level.

1. Procure your new high-end PC or low-end server based on the minimum requirements specified in **Section 1 Remote – Client Technical Specifications**
2. Configure your new hardware to the specifications documented within **Section 1**
3. Ensure that the new machine has the same local admin account as the old machine. If this changes, please provide the new account information to FirstWatch Technical Support.
4. Configure Remote Access on the new machine for FirstWatch access using the same method as the old machine (e.g. WebEx Remote Access, RDP, VNC etc...) If you are currently using WebEx Remote Access, contact FirstWatch to obtain the instructions for reinstalling on the new machine. If your company's remote access method changes, please notify FirstWatch Technical Support of the change. After remote connectivity has been installed, call FirstWatch Support so that they can validate and test the connection remotely.
5. Provide the new machine name and IP address to FirstWatch Support along with any new credentials.
6. Create a new ODBC System DSN connection on new machine using the same naming convention and credentials as the old machine. Ensure that it is directed to the same database as the old machine and test the connectivity.
7. Copy the entire "FirstWatch64" directory from the old machine to the new. This is typically located on the root of C:\ however it varies depending on your configuration.
8. **ProQA Customers Only**: If your system is configured to send ProQA files to the FirstWatch Server, you need to change the export path on one of the workstations in the ProQA admin utility to output the files to the designated ProQA share on the new machine using the same method as the old. Please contact FirstWatch Support if you require the ProQA FirstWatch Export Activation Instructions.

Once you've completed the preparation steps, please contact FirstWatch Support so that we can proceed with our scheduled reinstallation time and complete the transition process. Once we can successfully connect remotely, the amount of time to reconfigure the new machine will take approximately 15-30 minutes. The final steps will include stopping the services on the old machine and starting them on the new machine.

FIRST WATCH

Every Record. In Real Time. Automatically.

To contact FirstWatch Operations and Support, call 760-943-9123 ext. 255 or email support@firstwatch.net.

Statement of Work

El Dorado County
Emergency Medical Services Agency

FirstWatch System –Real Time Monitoring & Alert System

Document Control

Change Control

Document Name	Statement of Work
Reference	FirstWatch – Real Time Monitoring & Alert System
File Name	El Dorado County EMS Agency – FirstWatch Statement of Work.doc

Ver.	Date	File Name	Details	Author
1.0	10/18/21	El Dorado County EMS Agency – FirstWatch Statement of Work.doc	Draft 1	Katelyn Gilligan

Table of Contents

1. Introduction

This Statement of Work defines the framework of deliverables for this Project in terms of products, equipment, and services and establishes standards for the deliverables, which may be further refined through additional documents.

Within this document, 1) “FirstWatch” refers to FirstWatch Solutions, Inc; 2) “Client” refers to El Dorado County Emergency Medical Services Agency.

1.1 Defined Terms

- The word “FirstWatch” to mean FirstWatch Solutions, Inc.
- The word “Client” to mean El Dorado County Emergency Medical Services Agency.
- The word “Days” to mean Business Days.
- The word “Software” to mean the code installed locally on the Client’s server to retrieve and transmit data between systems.
- The word “Information” to mean confidential patient, private, or trade secret data.
- The word “System” to mean the hardware components that have been carefully chosen so that they work well together, and software components or programs that run in the computer.
- The words “Work”, “Services”, “Program”, or “Project” to mean all matters and things required to be done by Client in accordance with the provisions of the Statement of Work.
- The word “Trigger” to mean a representation of data based on a set of user-defined data filter criteria using one or more of the Client’s requested analytical methods for a specific data source.
- The word “All Responses” to mean an unfiltered trigger view of every call within Client’s CAD data source(s).
- The word “All electronic patient care reporting (ePCR)” to mean an unfiltered trigger view of every record within Client’s ImageTrend ePCR data source.
- The word “Go Live” to mean receiving and processing data through the FirstWatch system with subscribed users for live operations against the initial “All Calls” Trigger.
- The word “Lead” to mean to main point of contact at the FirstWatch or Client site.
- The word “Wholesale” to mean extensive or large-scale rework.

1.2 Introduction

FirstWatch shall provide all professional services and software necessary to meet the requirements of this Statement of Work. FirstWatch shall appoint a Project Manager as the principal contact who is responsible for implementing this project within the framework of the Statement of Work. The FirstWatch Project Manager organizes a team of specialists assigned to the project from FirstWatch. FirstWatch’s Project Manager shall manage each of these personnel to provide a coordinated implementation of the project defined by this Statement of Work.

Client will appoint a Contract Administrator as the Client's principal contact to manage a team of personnel designated to contribute to the implementation of this project. Similar to the duties of FirstWatch's Project Manager, the Client's Contract Administrator has overall responsibility to manage the other members of the Client's team. This Statement of Work includes an overview of the Client's responsibilities.

2. Scope

2.1 FirstWatch Project Overview

The FirstWatch project schedule is summarized at the end of this Statement of Work. A detailed project schedule shall be finalized after consulting the Client about the availability of the Client's personnel and responsibilities. Assuming prompt and diligent activities by the Client and FirstWatch, the estimated project timeline from contract execution and project initiation payment to "Go Live" is estimated to be six (6) weeks. This estimate is based upon the current and past experience and on availability of FirstWatch and Client resources.

The term "Go Live" shall mean receiving and processing data through the FirstWatch system with subscribed users for live operations against the initial "All Calls" Trigger(s). The actual "Go Live" date may be revised by FirstWatch's Project Manager and Client's Contract Administrator based on feedback from project resources and system stabilization. Changes proposed by the Client in software or hardware configuration or the scheduling of meetings or training sessions may result in revisions to project chronology.

2.2 Scope Inclusions

This project includes the following deliverables:

- **System License for (DS1) – ImageTrend ePCR**

  This interface allows the FirstWatch system to monitor ePCR data hosted by ImageTrend via a data feed from ImageTrend directly to FirstWatch. Adding ImageTrend electronic patient care records for Client will enhance the Client's view related to monitoring Quality Assurance and Quality Indicators and the impact of treatment related to improving patient outcomes. The data will be made available and linked to the other data sources described in this document through the FirstWatch web portal via FirstWatch Triggers and/or in the form of automated alerting where applicable.

- **System License for (DS2) – CALFIRE Northrup Grumman Computer Aided Dispatch (CAD), located in Camino as part of the Amador-El Dorado Unit**

  Data Source Integration Services – work to be performed to integrate the monitoring of the CAD Data into the FirstWatch system includes the installation and configuration of the necessary FirstWatch applications services to query, compress, encrypt and securely transmit data packets through a secure connection –SSL/HTTPS to the FirstWatch Data Centers. The data shall be made available through the FirstWatch web portal via FirstWatch Triggers and/or in the form of automated alerting where applicable.

- **System License for (DS3) – South Lake Tahoe Dispatch CAD**

  It is important to note that currently, South Lake Tahoe is dispatched off an existing Cyrun CAD. Within the next nine (9) to twelve (12) months, South Lake Tahoe will be converting from Cyrun CAD to SunRidge RIMS CAD which could result in a data source conversion. FirstWatch and Client will need to determine which CAD FirstWatch will integrate with at the time of contract execution. If FirstWatch integrates with the existing Cyrun CAD, there could potentially be costs associated with a data source conversion to SunRidge RIMS CAD.

  Data Source Integration Services – work to be performed to integrate the monitoring of the CAD Data into the FirstWatch system includes the installation and configuration of the necessary FirstWatch applications services to query, compress, encrypt and securely transmit data packets through a secure connection –SSL/HTTPS to the FirstWatch Data Centers. The data shall be made available through the FirstWatch web portal via FirstWatch Triggers and/or in the form of automated alerting where applicable.

- **FirstWatch System All Responses and All ePCR Triggers**

  Upon successful completion of the data transmissions to the FirstWatch Data Centers, FirstWatch shall develop All Responses and All ePCR Triggers which are generally an unfiltered Trigger view for processing all of the CAD and ePCR incidents that are entered into the Client’s data sources. The FirstWatch All Responses and All ePCR Triggers shall be made available to only authorized users of the FirstWatch system as dictated by the Client’s Contract Administrator.

- **Twenty (20) Included Standard FirstWatch Triggers**

  FirstWatch and the Client will work in a collaborative manner to define the necessary Standard FirstWatch Triggers as defined by the Client and within the scope of a Standard FirstWatch Trigger.

- **Ten (10) Custom Report Development Hours for APOT**

  An Ambulance Patient Offload Times (APOT) report shall be developed against the same data that FirstWatch will be pulling and analyzing from Client’s CAD or ePCR data for APOT. Reports offer users the ability to define specific and unique case views of data in a way which makes sense for Client. Through the use of SQL Reporting Services, FirstWatch can automate the delivery of report data to defined organization users and groups. The reports can be exported or delivered in various formats including Excel, Word, PDF, HTML, XML, and CSV.

- **One (1) Interactive Data Visualization Modules (IDV)**

  FirstWatch Interactive Data Visualization Tool (IDV) is a modernized look and feel that allows Client to interact with the data that has been configured for a particular trigger. Client is able to view or filter based upon the desired data elements and has the ability to:

  - search through filter criteria or apply and save custom filters to the Client's profile
  - select data ranges, demographically, day of week/hour of day, station, company, shift, battalion, or unit
  - have the ability to group multiple data elements and compare to previous day, month, or year

- **Online Compliance Utility Module (OCU)**

  OCU is a queue-based module used to help El Dorado County EMS Agency and the provider agencies manage contractual performance & response time compliance through a web-based utility.

- **FirstPass Module**

  FirstPass is near real-time clinical measurement and protocol monitoring tool designed to watch for deviations in expected treatments to medical protocols. Web based and flexible in design, FirstPass is a workflow driven tool that is highly customizable to meet the unique needs of the various stakeholders throughout the organization with access anywhere there is Internet connectivity. The goal of FirstPass is to get critical information into the hands of key stakeholders as soon as possible related to patient care outcomes and expected results.

2.3 Scope Exclusions

Any Client requests for work or items not described in this Statement of Work, including but not limited to custom software, are not included in this project. In such cases, these items can be added through a fully executed Amendment.

2.4 Project Personnel

- **Project Management**

  FirstWatch shall assign a dedicated Project Manager to manage all aspects of the project through project deliverables. The FirstWatch Project Manager will coordinate efforts related to project tasks with the Client's Contract Administrator and FirstWatch team members.

- **Operations and Support**

  The FirstWatch Operations and Support team shall work with the FirstWatch Project Manager on the completion of project tasks.

- **Engineering**

  The FirstWatch Engineering team shall work with the Operations and Support team to develop install and develop necessary software requirements to meet the project deliverable objectives.

2.5 Project Assumptions and Limitations

- The Client will be responsible for connecting FirstWatch with personnel at ImageTrend and providing access to Client's CALFIRE Northrup Grumman CAD, located in Camino as part of the Amador-El Dorado Unit, and South Lake Tahoe Dispatch's CAD databases as specified in this Statement of Work.
- The Client will assign a Contract Administrator or other "Lead" person as a single Point of Contact for the duration of the project.
- Once data from the Primary Data Source (DS1) is available and the Acceptance Test Plan (ATP) is completed by the Client, FirstWatch shall help the Client identify pertinent triggers and then shall define and develop those triggers and when completed shalll subscribe authorized Client users to the applicable triggers and notifications.

2.6 Project Issues and Risks

- **Software Issues**

  Software related issues shall be managed in accordance with the Client's FirstWatch System Maintenance Services, which can be provided at Client's request.

- **Project Risks**
  - **Project Meetings and Tasks**

    Changes proposed in the scheduling of meetings, training sessions, or project related tasks may result in project timeline revisions.

  - **Hardware, Software, and Third-Party Configuration**

    Changes in the proposed hardware, software, or third-party configuration changes may result in project timeline revisions.

2.7 Overview of Client Responsibilities

Client responsibilities are identified in Exhibit A, marked “FirstWatch Remote Client Installation Guide,” incorporated herein and made by reference a part hereof. Exhibit A provides implementation requirements and actions to be performed by the Client and its staff during the data source implementation phase of the project. Such items include but are not limited to – Network and Cabling needs, Training Facilities, Technical Support connectivity (Virtual Private Network [VPN] or Integrated Services Digital Network [ISD]N) and physical requirements for the equipment facility.

FirstWatch’s Project Manager and the Client Contract Administrator will work closely to revise as necessary and mutually agree upon the on-going client responsibilities that are specific to this project.

FirstWatch Equipment & Configuration Overview

The Client will provide all equipment and third-party software for this project. The Client will provide a Read-Only account for accessing CAD data against the CALFIRE Northrup Grumman and South Lake Tahoe Dispatch CAD databases. The FirstWatch Data Exporter shall connect to the specified CAD database using the Read-Only account provided by the Client via Open Database Connectivity (ODBC) or other agreed to connectivity.

Client will notify FirstWatch and ImageTrend once the Client is ready to proceed with the ImageTrend to FirstWatch interface. FirstWatch and ImageTrend shall implement the standard interface to securely transmit and receive the ePCR records for this project.

3 Professional Services

3.1 Project Management

FirstWatch shall appoint a Project Manager with the authority to make certain decisions relevant to the project and have direct access to FirstWatch’s executive management for resolving problems beyond the Project Manager's immediate authority.

The Project Manager shall coordinate with Client's Contract Administrator through scheduled meetings, create the project plan and project schedule, review the project and its progress, and review the current task list and upcoming milestones. The FirstWatch Project Manager shall manage the implementation plan and team members who will be associated with the project.

3.2 FirstWatch User/System Training

Training on the FirstWatch System is currently accomplished remotely via WebEx-powered Internet-based meetings.

Users who require training shall receive it via a scheduled online training session with FirstWatch Operations personnel.

All that is required for the training webinar is an Internet-connected personal computer (PC) and telephone. Training is best accomplished in an area where all participants can see the monitor/screen and hear and ask questions to the FirstWatch Instructor.

Training topics include information on the basic understanding of data monitoring, and how to use and access the FirstWatch System.

3.3 Trigger Definition, Re-definition, & Refinement

FirstWatch shall work with the Client to make complete “Wholesale” changes to each Trigger up to twice per Trigger, per year, and as many minor refinements to existing triggers as the Client reasonably requires per year.

3.4 Project Meetings

Project implementation shall involve various meetings to manage project activities. These include, but are not necessarily limited to, the following required sessions:

- Initial technical discussion related to data access for the Computer Aided Dispatch and ePCR data sources
- Trigger definition discussions
- System user access discussions
- Project status update conference calls

3.5 Installation Tasks

- The Client will ensure that remote access is available to the existing FirstWatch server.
- The Client will ensure that a Read-Only (db_datareader & db_denydatawriter) account is created for FirstWatch on the database server that FirstWatch shall be monitoring for CAD. Ideally, the database that FirstWatch will be monitoring will be a near real-time replica of the production CAD database.
- The Client will create an ODBC data source name (DSN) connection on the existing FirstWatch server using the Read-Only account that was created for FirstWatch access to the CAD data source.
- Once data access has been provided, FirstWatch shall verify data connectivity and submit a ticket to FirstWatch’s project deployment queue for installation.
- FirstWatch deployment team shall remotely connect to the existing FirstWatch server to install the necessary FirstWatch software components to query the CAD data source at predetermined intervals. The default query frequency for CAD is sixty (60) seconds. If the Client desires a query frequency of greater than sixty (60) seconds, the Client will specify their requested frequency level. This will effectively create a new instance of the FirstWatch Data Exporter on the existing FirstWatch server for monitoring the CAD data source.

- The Client will notify FirstWatch and ImageTrend once the Client is ready to proceed with the ImageTrend to FirstWatch NEMSIS 3.4 ePCR interface. FirstWatch and ImageTrend shall implement the standard interface to securely transmit and receive the ePCR records for this project.
- Once the FirstWatch Data Exporter is installed and CAD and ePCR data is flowing, FirstWatch shall develop “All Responses” and “All ePCR” Triggers and pull a one (1) year baseline of historical data for trending analysis. If additional historical data is required, FirstWatch and Client will need to work with the data source vendors to request the data.
- FirstWatch shall obtain a list of approved subscribers for the “All Responses” and “All ePCR Triggers”, create new users or subscribe existing users to the Triggers, and notify the Client upon completion.

3.6 Client Responsibilities

The Client is responsible for (where applicable):

- Electrical facilities (e.g., outlets, generator, and other electrical infrastructure facilities).
- Cabling (e.g., power, network, interface, and other electrical and data transmission lines).
- Network/communications connections (e.g., wide area network [WAN], telephone, Integrated Services Digital Network [ISDN], VPN, and other voice/data connections), or ongoing network/communications charges associated with installation, operation or support of the proposed system.
- Configuration and/or programming of network routers, switches, and bridges.
- Training for third-party software.
- Computer workstations or mobile devices for accessing FirstWatch via the web portal or alerts.
- Participation in FirstWatch system training and Trigger definitions.
- Participation in project status update conference calls
- Making the appropriate personnel available for scheduled training sessions; and
- Internet access for training via WebEx sessions.

4 Overview of Project Implementation Schedule

Project Implementation occurs in several phases and requires numerous actions by the Client and FirstWatch. These activities are interdependent - sometimes requiring action by FirstWatch before the Client can proceed, and sometimes requiring action by the Client before FirstWatch can proceed. The following schedule overview identifies key tasks and their interdependencies.

Once the project commences, a detailed schedule will be developed for full project implementation. Such a project schedule will be under continuous evolution, as adjustments need to be made in the course of the project. It’s important to note that for some activities, such as training or interface integration; a several day delay may result in a several week project timeline revision as resources for both the Client and for FirstWatch may need rescheduling.

4.1 Project Initiation Phase

Project Initiation is the phase of the project used to 'introduce' the applicable FirstWatch (FW) and Client team members in the project, develop a project schedule, conduct initial consultation and information gathering sessions, and to prepare the Client site for deployment. This phase can take numerous days, depending upon the availability of resources to review and comment on documents. Major tasks include the following:

Task	Responsibility
Initiation Phase	
Complete Project Confirmation	
Authorize Project / PO	Client
Send Licensing Documentation (if applicable)	FW
Sign Licensing / Maintenance Agreement (if applicable)	FW, Client
Complete Kick-Off Meeting	
Schedule Kick-Off Meeting	FW, Client
Review General Project Flow	FW, Client
Identify All Stakeholders	FW, Client
Complete Demo (if desired)	FW, Client
Complete Technical Meeting	
Request detailed printout example of data source reports and data dictionary if available	FW
Send WebEx Remote Access Install Guide (if applicable)	FW
Send FW Remote Install Guide (if applicable)	FW
Schedule Technical Discussion Meeting	FW, Client
Complete Technical Discussion Mtg. Agenda	
Discuss ODBC / Web Services Approach	FW, Client
Review Project Technical Requirements	FW, Client
Review Deployment Process	FW, Client
Complete Technical Discussion Meeting	FW, Client

4.2 Deployment Phase

The deployment phase of the project is used to prepare the local deployment site, validate hardware, software and network connectivity and Go Live with the initial FirstWatch system's All Responses and All ePCR Triggers. Major tasks include the following:

Deployment Phase	
Prepare Install Site	
Receive detailed printout example of data source Report	FW
Order Server (if applicable, or VM server, existing server or workstation)	Client
Receive Server (if applicable)	Client
Prepare Server (Notify FW of Readiness)	Client
Validate Hardware Configuration/Connectivity	
Provide technical configuration/connectivity information	Client
Test connectivity	FW
Add to Master Reference File	FW
Install Data Sources	
Move Project to FW Deployment Queue	FW
Complete Development of All Responses / All ePCR Triggers	FW
QA All Responses / All ePCR Triggers	FW
Subscribe Users to All Responses / All ePCR Triggers (System LIVE)	FW

4.3 Completion Phase

The completion phase consists of system training and project wrap up tasks. Major tasks include the following:

Completion Phase	
Complete Training	
Schedule System Overview / Orientation	FW, Client
Complete System Overview / Orientation	FW, Client
Create Report	
Finalize Milestones and Dates	FW
Document Maintenance Components	FW
Re-assess project for final completion	FW
Promote Project to FW Support	FW

4.4 Post Implementation Phase

The post implementation phase consists of Trigger definition, development, and ongoing project support. At this stage, the Base Implementation will have been completed and the Client will be fully transitioned from FirstWatch Project Management into the Operations and Support team for further Trigger development and fine-tuning and implementation of enhancements.

Trigger Development (In Support)	
Define Triggers & Modules	FW, Client
Develop Triggers & Modules	FW
QA Triggers & Modules	FW, Client
Configure Std. Alert Methods for Triggers	FW, Client
Subscribe Alert Recipients for Triggers	FW
Subscribe Users to Triggers & Modules	FW

END OF DOCUMENT