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 undersigned software user ("Client" or "Agency"). This Agreement is effective as of the _____ day of ___________________________, 2021 ("Effective Date") for a term of five (5) years ending on the _____ day of ___________________, 2026 unless terminated earlier in accordance with Paragraph 12 of this Agreement.

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, and to pay a late fee of one and a half percent (1.5%) interest per month on all overdue amounts for any fees due and payable under the Agreement. 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. 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. *Termination.* Either party may terminate this Agreement if there is a material breach by either party that is not cured within thirty (30) days after receipt of written notice of such breach. Upon termination of this Agreement, Client shall promptly discontinue using the Software and return to FirstWatch, or certify in writing, the destruction of all Software, Documentation, and FirstWatch training materials.

13. Insurance Provisions

Insurance. FIRSTWATCH shall obtain and maintain in full force and effect throughout the term of this Agreement, and thereafter as to matters occurring during the term of this Agreement, the following insurance coverage:

(a)Workers' Compensation Insurance. To the extent required by law during the term of this Agreement, FIRSTWATCH shall provide workers' compensation insurance for the performance of any of FIRSTWATCH's duties under this Agreement, including but not limited to, coverage for workers' compensation and employer's liability and a waiver of subrogation, and shall provide CLIENT with certification of all such coverages upon request by CLIENT's Risk Manager.

(b)Liability Insurance. FIRSTWATCH shall obtain and maintain in full force and effect during the term of this Agreement the following liability insurance coverages, issued by a company admitted to do business in California and having an A.M. Best rating of A:VII or better, or equivalent self-insurance:

(1)General Liability. Commercial general liability [CGL] insurance coverage (personal injury and property damage) of not less than ONE MILLION DOLLARS ($1,000,000) combined single limit per occurrence, covering liability or claims for any personal injury, including death, to any person and/or damage to the property of any person arising from the acts or omissions of FIRSTWATCH or any officer, agent, or employee of FIRSTWATCH under this Agreement. If the coverage includes an aggregate limit, the aggregate limit shall be no less than twice the per occurrence limit.

(2)Professional Liability/Errors and Omissions. Professional liability [or errors and omissions] insurance for all activities of FIRSTWATCH arising out of or in connection with this Agreement in an amount not less than ONE MILLION DOLLARS ($1,000,000) per claim.

(3)Comprehensive Automobile Liability Insurance. Comprehensive automobile liability insurance (Bodily Injury and Property Damage) on owned, hired, leased and non-owned vehicles used in conjunction with FIRSTWATCH's business of not less than ONE MILLION DOLLARS ($1,000,000) combined single limit per occurrence. Coverage shall be business auto insurance coverage using Insurance Services Office (ISO) form number CA 0001 06 92 including symbol 1 (any Auto) or the exact equivalent. If FIRSTWATCH owns no vehicles, this requirement may be satisfied by a non-owned auto endorsement to the General Liability Insurance described in subparagraph (b)(1) above. If FIRSTWATCH or FIRSTWATCH's employees, officers, or agents will use personal automobiles in any way in the performance of this Agreement, FIRSTWATCH shall provide evidence of personal auto liability coverage for each such person upon request.

(c)Certificates of Coverage. All insurance coverages referenced in 2.7(b), above, shall be evidenced by one or more certificates of coverage or, with the consent of CLIENT's Risk Manager, demonstrated by other evidence of coverage acceptable to CLIENT's Risk Manager, which shall be filed by FIRSTWATCH with the Health and Human Services Agency prior to commencement of performance of any of FIRSTWATCH's duties.

(1)The certificate(s) or other evidence of coverage shall reference this Agreement by its CLIENT number or title and department; shall be kept current during the term of this Agreement; shall provide that CLIENT shall be given no less than thirty (30) days prior written notice of any non-renewal, cancellation, other termination, or material change, except that only ten (10) days prior written notice shall be required where the cause of non-renewal or cancellation is non-payment of premium; and shall provide that the inclusion of more than one insured shall not operate to impair the rights of one insured against another insured, the coverage afforded applying as though separate policies had been issued to each insured, but the inclusion of more than one insured shall not operate to increase the limits of the company's liability.

(2)Waiver of Subrogation and Additional Insured Endorsements. For the commercial general liability insurance coverage referenced in 2.7(b)(1) and, for the comprehensive automobile liability insurance coverage referenced in 2.7(b)(3) where the vehicles are covered by a commercial policy rather than a personal policy, FIRSTWATCH shall also file with the evidence of coverage an endorsement from the insurance provider naming CLIENT, its officers, employees, agents and volunteers as additional insureds and waiving subrogation. For the Workers Compensation insurance coverage, FIRSTWATCH shall file with the evidence of coverage an endorsement waiving subrogation.

(3)The certificate or other evidence of coverage shall provide that if the same policy applies to activities of FIRSTWATCH not covered by this Agreement, then the limits in the applicable certificate relating to the additional insured coverage of CLIENT shall pertain only to liability for activities of FIRSTWATCH under this Agreement, and that the insurance provided is primary coverage to CLIENT with respect to any insurance or self-insurance programs maintained by CLIENT. The additional insured endorsements for the general liability coverage shall use Insurance Services Office (ISO) Form No. CG 20 09 11 85 or CG 20 10 11 85, or equivalent, including (if used together) CG 2010 10 01 and CG 2037 10 01; but shall not use the following forms: CG 20 10 10 93 or 03 94.

(4)Upon request by CLIENT's Risk Manager, FIRSTWATCH shall provide or arrange for the insurer to provide within thirty (30) days of the request, certified copies of the actual insurance policies or relevant portions thereof.

(d)Deductibles/Retentions. Any deductibles or self-insured retentions shall be declared to, and be subject to approval by, CLIENT's Risk Manager, which approval shall not be denied unless the CLIENT's Risk Manager determines that the deductibles or self-insured retentions are unreasonably large in relation to compensation payable under this Agreement and the risks of liability associated with the activities required of FIRSTWATCH by this Agreement. At the option of and upon request by CLIENT's Risk Manager if the Risk Manager determines that such deductibles or retentions are unreasonably high, either the insurer shall reduce or eliminate such deductibles or self-insurance retentions as respects CLIENT, its officers, employees, agents and volunteers or FIRSTWATCH shall procure a bond guaranteeing payment of losses and related investigations, claims administration and defense expenses.

(e)Inclusion in Subcontracts. FIRSTWATCH agrees to require all subcontractors and any other entity or person who is involved in providing services under this Agreement to comply with the Workers Compensation and General Liability insurance requirements set forth in this Paragraph 2.7.

(f)Failure to demand evidence of full compliance with the insurance requirements set forth in this Agreement or failure to identify any insurance deficiency shall not relieve FIRSTWATCH, nor be construed or deemed a waiver of, its obligation to maintain the required insurance at all times during the performance of this Agreement.

14. *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 cooperate, 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-year depreciation basis. This agreement states the entire liability of FirstWatch with respect to third party claims of intellectual property infringement.

15. *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.

16. *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.

17. *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.

18. *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. *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.

SIGNATURE PAGE FOLLOWS

AGREED AND ACCEPTED:

FirstWatch Solutions, Inc.

Date: 10/07/2021

By:__________________
TODD STOUT, President

Client Name and Address:

Napa County Health and Human Services Agency
2751 Napa Valley Corporate Drive, Bldg. B
Napa, CA, 94558

Date:__________________

By:__________________
ALFREDO PEDROZA
Title: Chair, Board of Supervisors

APPROVED AS TO FORM
Office of County Counsel

By: _____**Rachel L. Ross (e-signature)**

Date:______**10/06/21**__________

Deputy County Counsel

Date: APPROVED BY THE NAPA COUNTY BOARD OF SUPERVISORS

Date:

Processed By: __________________

Deputy Clerk of the Board
ATTEST: NEHA HOSKINS
Clerk of the Board of Supervisors

By: __________________
Date:__________________

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 PC/Server

    - All data integration with Client's Data Source/System integrated via:
        - Connectivity to a data source via ODBC or similar means;
        - or Text or XML ***file*** output for each incident from a Client-provided process (one 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 – Intergraph CAD)	1	$20,381	$20,381
2	Annual Support & Maintenance* (DS1)	1	$4,483.82	$4,483.82
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 – ePCR (vendor to be determined by provider)	1	$14,267	$14,267
7	Annual Support & Maintenance* (DS2)	1	$3,138.74	$3,138.74
8	Data Source Integration (DS2)	1	$7,500	$7,500
9	Standard System Triggers (included)	20	Incl.	Incl.
10	Interactive Data Visualization Module (IDV)	1	Incl.	Incl.
11	Online Compliance Utility Module (OCU)	1	$30,000	$30,000
12	Online Compliance Utility Annual Support & Maintenance	1	$6,600	$6,600
13	FirstPass Module (FP)	1	$30,000	$30,000
14	FirstPass Annual Support & Maintenance	1	$6,600	$6,600
15			**Total Price**	**$142,470.56**

* License and Maintenance costs are for monitoring Napa County Health & Human Services' EMS Calls. Assumptions are based on 15,000 annual incidents, and include a 'buffer' of plus or minus (±) 20% of the call volume.

"Client" FirstWatch Payment Schedule	
Project Initiation Payment: 50% >Invoiced for at Contract Execution	$71,235.28
FirstWatch Base System (DS1) Installation Payment: 40% >Invoiced for at Base System Installation	$56,988.22
FirstWatch Base System (DS1) Acceptance Payment: 10% >Invoiced for at Base System Acceptance (ATP)	$14,247.06

Maintenance fees beyond the Term of this Agreement (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 3% per year.

Estimated Annual Support & Maintenance for Year 2	$21,447.24
Estimated Annual Support & Maintenance for Year 3	$22,090.65
Estimated Annual Support & Maintenance for Year 4	$22,753.37
Estimated Annual Support & Maintenance for Year 5	$23,435.97

Switching Data Sources against a "LIVE" OCU and/or FirstPass Module(s): Timing and Financial Considerations

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

*OCU Module

When customer 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 customers 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 customer has OCU live under one response time compliance contract, and their response time compliance contract requirements are changed such that the OCU must be changed, there will be a Contract Re-Configuration Fee of up to $6,000.

*FirstPass Module

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

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	M Shaun Vincent Emergency Medical Services Administrator Napa County Health & Human Services 2751 Napa Valley Corporate Drive, Bldg. B Napa, CA 94558	Phone : 707-299-2155 Email : michael.vincent@countyofnapa.org

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.

Schedule B:

FirstWatch Solutions, Inc.
Business Associate Agreement
Between FirstWatch Solutions, Inc. and Napa County Health & Human Services

This Exhibit shall constitute the Business Associate Agreement (the "Agreement") between **FirstWatch Solutions, Inc.,** (the "Business Associate") and Napa County (the "Covered Entity"), and applies to the functions Business Associate will perform on behalf of Covered Entity (collectively, "Services"), that are identified in the Master Agreement (as defined below).

1.**Purpose.** This Agreement is intended to ensure that the Business Associate will establish and implement appropriate privacy and security safeguards with respect to "Protected Health Information" (as defined below) that the Business Associate may create, receive, maintain, transmit, use, or disclose in connection with the Services to be provided by the Business Associate to the Covered Entity, and that such safeguards will be consistent with the standards set forth in regulations promulgated under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") as amended by the Health Information Technology for Economic and Clinical Health Act as set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 ("HITECH Act").

2.**Regulatory References.** All references to regulatory Sections, Parts and Subparts in this Agreement are to Title 45 of the Code of Federal Regulations as in effect or as amended, and for which compliance is required, unless otherwise specified.

3. **Definitions.** Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms are defined in Sections 160.103, 164.304 and 164.501.

(a) Business Associate. "Business Associate" shall mean the party identified above as the "Business Associate".

(b) Breach. "Breach" shall have the same meaning as the term "breach" in Section 164.402.

(c) Covered Entity. "Covered Entity" shall mean the County of Napa, a hybrid entity, and its designated covered components, which are subject to the HIPAA Rules.

(d) Designated Record Set. "Designated Record Set" shall have the same meaning as the term "designated record set" in Section 164.501.

(e) Electronic Media. "Electronic Media" shall have the same meaning as the term is defined in Section 160.103.

(f) Electronic Protected Health Information. "Electronic Protected Health Information" ("EPHI") is a subset of Protected Health Information and means individually identifiable health information that is transmitted or maintained in electronic media, limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

(g) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(h) Individual. "Individual" shall have the same meaning as the term "Individual" in Section 164.501 and shall include a person who qualifies as a personal representative in accordance with Section 164.502(g).

(i) Master Agreement. "Master Agreement" shall mean the contract or other agreement to which this Exhibit is attached and made a part of.

(j) Minimum Necessary. "Minimum Necessary" shall mean the minimum amount of Protected Health Information necessary for the intended purpose, as set forth at Sections

164.502(b) & 164.514(d): *Standard: Minimum Necessary.*

(k) Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at Part 160 and Part 164, Subparts A and E.

(l) Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in Section 160.103, limited to the information received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

(m) Required By Law. "Required by law" shall have the same meaning as the term "required by law" in Section 164.103.

(n) Secretary. "Secretary" shall mean the Secretary of the United States Department of Health and Human Services ("DHHS") or his/her designee.

(o) Security Incident. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of personally identifiable information. A Security Incident includes the attempted or successful unauthorized access, use, disclosure, modification, or destruction of or interference with systems operations in an information system which processes Protected Health Information that is under the control of Covered Entity, or Business Associate of Covered Entity, but does not include minor incidents that occur on a daily basis, such as scans, "pings", or unsuccessful random attempts to penetrate computer networks or servers maintained by Business Associate.

(p) Security Rule. "Security Rule" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

(q) Subcontractor. "Subcontractor" means a subcontractor of Business Associate that creates, receives, maintains, or transmits Protected Health Information on behalf of the Business Associate.

(r) Unsecured Protected Health Information. "Unsecured Protected Health Information" shall have the same meaning as the term "unsecured protected health information" in Section 164.402, limited to the information received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

4. Business Associate's Obligations and Compliance with the HIPAA Privacy and Security Rules.

(a) Business Associate acknowledges that it is directly required to comply with the HIPAA Rules and that Business Associate (including its subcontractors) may be held directly liable and subject to penalties for failure to comply. To the extent the Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 CFR Part 164 of the Privacy Rule, Business Associate agrees to comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligations.

(b) Business Associate agrees not to use or further disclose Protected Health Information other than as permitted or required by this Agreement, or as required by law.

(c) Business Associate shall not sell Protected Health Information.

5. Permitted Uses and Disclosures.

(a) Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity for the purposes specified in Attachment 1 to this Exhibit, which if completed and attached hereto is incorporated by reference, or as otherwise specified in the Master Agreement, subject to limiting use and disclosure to applicable minimum necessary rules, regulations and statutes and provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity. Business Associate must make reasonable efforts to limit Protected Health Information to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request.

(b) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

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

(d) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by Section 164.504(e)(2)(i)(B).

(e) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities consistent with Section 164.502(j).

(f) Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 of the Privacy Rule if done by Covered Entity, except for the specific uses and disclosures set forth herein.

6.**Appropriate Safeguards.**

(a) Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Health Information that is created, received, maintained or transmitted on behalf of the Covered Entity and limiting use and disclosure to the Minimum Necessary.

(b) Safeguarding Electronic Protected Health Information. Business Associate agrees to comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information. Business Associate must secure all Electronic Protected Health Information by technological means that render such information unusable, unreadable, or indecipherable to unauthorized individuals and in accordance with the National Institute of Standards Technology (NIST) Standards and Federal Information Processing Standards (FIPS) as applicable, Should Business Associate fail to comply with this provision, it agrees to hold harmless, defend at its own expense and indemnify Covered Entity in accordance with the terms of Section 9 of the Agreement, "Indemnification".

(c) Destruction of Protected Health Information on paper, film, or other hard copy media must involve either shredding or otherwise destroying the Protected Health Information so that it cannot be read or reconstructed.

(d) Should any employee or subcontractor of Business Associate have direct, authorized access to computer systems of Covered Entity that contain Protected Health Information, Business Associate shall immediately notify Covered Entity of any change of such personnel (e.g. employee or subcontractor termination, or change in assignment where such access is no longer necessary) in order for Covered Entity to disable the previously authorized access.

7.**Reporting Unauthorized Uses and Disclosures.**

(a) Business Associate agrees to notify Covered Entity of any access, use or disclosure of Protected Health Information not permitted or provided for by the Agreement of which it becomes aware, including any breach as required at Section 164.410, or security incident,. Such notification will be made immediately after discovery by telephone call at 707.253.4715, plus e-mail at Privacy.Officer@countyofnapa.org, and will include, to the extent possible, the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used or disclosed, a description of the Protected Health Information involved, the nature of the unauthorized access, use or disclosure, the date of occurrence, and a description of any remedial action taken or proposed to be taken by Business Associate. Business Associate will also provide to Covered Entity any other available information that the Covered Entity is required to include in its notification to the Individual under Section 164.404(c) at the time of the initial report or promptly thereafter as the information becomes available.

(b) In the event of a request by law enforcement under Section 164.412, Business Associate may delay notifying Covered Entity for the applicable timeframe.

(c) A breach or unauthorized access, use, or disclosure shall be treated as discovered by the Business Associate on the first day on which such unauthorized access, use, or disclosure is known, or should reasonably have been known, to the Business Associate or to any person, other than the individual committing the unauthorized disclosure, that is an employee, officer, subcontractor, agent or other representative of the Business Associate.

(d) In meeting its obligations under this section, it is understood that Business Associate is not acting as the Covered Entity's agent. In performance of the work, duties, and obligations and in the exercise of the rights granted under this Agreement, it is understood and agreed that Business Associate is at all times acting as an independent contractor in providing services pursuant to this Agreement and the Master Agreement.

8. **Mitigating the Effect of a Breach, Security Incident, or Unauthorized Access, Use or Disclosure of Unsecured Protected Health Information.**

(a) Business Associate agrees to mitigate, to the greatest extent possible, any harm that results from the breach, security incident, or unauthorized access, use or disclosure of Unsecured Protected Health Information by Business Associate or its employees, officers, subcontractors, agents, or other representatives.

(b) Following a breach, security incident, or any unauthorized access, use or disclosure of Unsecured Protected Health Information, Business Associate agrees to take any and all corrective action necessary to prevent recurrence, to document any such action, and to make this documentation available to Covered Entity.

(c) Except as required by law, Business Associate agrees that it will not inform any third party of a breach or unauthorized access, use or disclosure of Unsecured Protected Health Information without obtaining the Covered Entity's prior written consent. Covered Entity hereby reserves the sole right to determine whether and how such notice is to be provided to any Individuals, regulatory agencies, or others as may be required by law, regulation or contract terms, as well as the contents of such notice. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, Business Associate shall cooperate with and coordinate with Covered Entity to ensure such reporting is in compliance with applicable law and to prevent duplicate reporting, and to determine responsibilities for reporting.

9. **Indemnification.**

(a) Business Associate agrees to hold harmless, defend at its own expense, and indemnify Covered Entity for the costs of any mitigation undertaken by Business Associate pursuant to Section 8, above.

(b) Business Associate agrees to assume responsibility for any and all costs associated with the Covered Entity's notification of Individuals affected by a breach or unauthorized access, use or disclosure by Business Associate or its employees, officers, subcontractors, agents or other representatives when such notification is required by any state or federal law or regulation, or under any applicable contract to which Covered Entity is a party.

(c) Business Associate agrees to hold harmless, defend at its own expense and indemnify Covered Entity, including Covered Entity's employees, directors, officers, subcontractors, agents or other members of its workforce (each of the foregoing hereinafter referred to as "Indemnified Party"), against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this Agreement or from any acts or omissions related to this Agreement by Business Associate or its employees, directors, officers, subcontractors, agents or other members of its workforce. Accordingly, on demand, Business Associate shall reimburse any Indemnified Party for any and all actual and direct losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party which results from the Business Associate's acts or omissions hereunder. Business Associate's obligation to indemnify any Indemnified Party shall survive the expiration or termination of this Agreement.

(d) Survival. The obligations of Business Associate under this Section 9 shall survive this Agreement.

10.**Individuals' Rights.**

(a) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by the Covered Entity, to Protected Health Information in a Designated Record Set, to
Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under
Section 164.524.

(b) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to make pursuant to Section 164.526, at the request of Covered Entity or an Individual, and in the time and manner designated by the Covered Entity.

(c) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an
Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.

(d) Business Associate agrees to provide to Covered Entity or an Individual, in the time and manner designated by Covered Entity, information collected in accordance with Section 10(c) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.

(e) Business Associate agrees to comply with any restriction to the use or disclosure of Protected Health Information that Covered Entity agrees to in accordance with Section 164.522.

11.**Obligations of Covered Entity.**

(a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with Section 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with Section 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

12.**Agents and Subcontractors of Business Associate.**

(a) Business Associate agrees to enter into written agreements with any agent, subcontractor or vendor, to whom it provides Protected Health Information received from Covered Entity or created, received , maintained or transmitted by Business Associate on behalf of Covered Entity, that impose the same restrictions, conditions and requirements that apply through this Agreement to Business Associate with respect to such information, including the requirement to immediately notify the Business Associate of any instances of any breach, security incident, intrusion , or unauthorized access to or use or disclosure of Protected Health Information of which it becomes aware. Upon request, Business Associate shall provide copies of such agreements to Covered Entity.

(b) Business Associate shall implement and maintain sanctions against any agent, subcontractor or other representative that violates such restrictions, conditions or requirements and shall mitigate the effects of any such violation.

13.**Audit, Inspection, and Enforcement.**

(a) Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity, available to any state or federal agency, including the Secretary, for the purposes of determining compliance with HIPAA and any related regulations or official guidance.

(b) With reasonable notice, Covered Entity and its authorized agents or contractors may audit and/or examine Business Associate's facilities, systems, policies, procedures, and documentation relating to the security and privacy of Protected Health Information to determine compliance with the terms of this Agreement. Business Associate shall promptly correct any violation of this Agreement found by Covered Entity and shall certify in writing that the correction has been made. Covered Entity's failure to detect any unsatisfactory practice does not constitute acceptance of the practice or a waiver of Covered Entity's enforcement rights under this Agreement.

14.**Permissible Requests by Covered Entity**. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

15.**Term and Termination.**

(a) The terms of this Agreement shall remain in effect for the duration of all services provided by Business Associate under the Master Agreement and for so long as Business Associate remains in possession of any Protected Health Information received from Covered Entity, or created, received, maintained or transmitted by Business Associate on behalf of Covered Entity unless Covered Entity has agreed in accordance with this Section 15 that it is not feasible to return or destroy all Protected Health Information.

(b) Upon termination of the Master Agreement, Business Associate shall recover any Protected Health Information relating to the Master Agreement and this Agreement in its possession and in the possession of its subcontractors, agents or representatives. Business Associate shall return to Covered Entity, or destroy with the consent of Covered Entity, all such Protected Health Information, in any form, in its possession and shall retain no copies.

(c) If Business Associate believes it is not feasible to return or destroy the Protected Health Information, Business Associate shall so notify Covered Entity in writing. The notification shall include: (1) a statement that the Business Associate has determined that it is not feasible to return or destroy the Protected Health Information in its possession, and (2) the specific reasons for such determination. Business Associate may retain only that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities. If Covered Entity agrees in its sole discretion that Business Associate cannot feasibly return or destroy the Protected Health Information, Business Associate shall ensure that any and all protections, requirements and restrictions contained in the Master Agreement and this Agreement shall be extended to any Protected Health Information for so long as Business Associate maintains such Protected Health Information, and that any further uses and/or disclosures will be limited to the purposes that make the return or destruction of the Protected Health Information infeasible.

(d) Covered entity may immediately terminate the Master Agreement if it determines that Business Associate has violated a material term of this Agreement.

(e) Survival. The obligations of Business Associate under this Section 15 shall survive this Agreement.

16.**Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the HIPAA Rules.

17.**Entire Agreement.** This Exhibit constitutes the entire HIPAA Business Associate Agreement between the parties, and supersedes any and all prior HIPAA Business Associate Agreements between them.

18.**Notices.**

(a) All notices required or authorized by this Agreement shall be in writing and shall be delivered in person or by deposit in the United States mail, by certified mail, postage prepaid, return receipt requested. Any notice sent by mail in the manner prescribed by this paragraph shall be deemed to have been received on the date noted on the return receipt or five days following the date of deposit, whichever is earlier.

(b) Any mailed notice, demand, request, consent, approval or communication that Covered Entity desires to give to Business Associate shall be addressed to Business Associate at the mailing address set forth in the Master Agreement.

(c) Any mailed notice, demand, request, consent, approval or communication that Business Associate desires to give to Covered Entity shall be addressed to Covered Entity at the following address:

Napa County Compliance and Privacy Officer
2751 Napa Valley Corporate Dr. Suite B
Napa, CA 94559
707.253-4715

(d) For purposes of subparagraphs (b) and (c) above, either party may change its address by notifying the other party of the change of address.

19.**Lost Revenues; Penalties/Fines.**

(a) Lost Revenues. Business Associate shall make Covered Entity whole for any revenues lost arising from an act or omission in billing practices by Business Associate.

(b) Penalties/Fines for Failure to Comply with HIPAA. Business Associate shall pay any penalty or fine assessed against Covered Entity arising from Business Associate's failure to comply with the obligations imposed by HIPAA.

(c) Penalties/Fines (other). Business Associate shall pay any penalty or fine assessed against Covered Entity arising from Business Associate's failure to comply with all applicable Federal or State Health Care Program Requirements, including, but not limited to any penalties or fines which may be assessed under a Federal or State False Claims Act provision.

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*

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