



FIRSTWATCH SOLUTIONS, INC. SOFTWARE LICENSE AGREEMENT

1. *Parties; Effective Date.* This Software License Agreement (“Agreement”) is between FirstWatch Solutions, Inc., 2035 Corte del Nogal, Suite 101, Carlsbad, California 92011 (“FirstWatch”) and the undersigned software user (“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, 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. *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.

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. *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.

19. *Venue.* Any action at law or in equity brought by either of the parties hereto for the purpose of enforcing a right or rights provided for by this Agreement shall be tried in a court of competent jurisdiction in the County of Riverside, State of California, and the parties hereby waive all provisions of law providing for a change of venue in such proceedings to any other county. In the event either party hereto shall bring suit to enforce any term of this Agreement or to recover any damages for and on account of the breach of any term or condition of this Agreement, it is mutually agreed that each party will bear their own attorney's fees and costs.

AGREED AND ACCEPTED:

FirstWatch Solutions, Inc.

Date: _____

By:  _____
Todd Stout (Nov 8, 2024 15:44 PST)

Name: Todd Stout, President

Client Name and Address:

City of Riverside and the Riverside Fire Department
3401 University Ave.
Riverside, CA 92501

Date: 11-13-2024

By: Steve McKinster

FirstWatch Solutions, Inc.

By: Marc Baker
Marc Baker (Nov 8, 2024 15:56 PST)

Print Name: Marc Baker

Title: Partner/VP & Corporate Secretary

Name: _____

Title: _____

By: _____
City Manager

Attest: _____
City Clerk

Certified as to Availability of Funds:

By: Jack Liu
Chief Financial Officer

Approved as to Form:

By: Jack Liu
Jack Liu (Nov 13, 2024 16:14 PST)
Interim City Attorney

Schedule A:

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

- If needed, single license of FirstWatch Thin-Client (Remote Data Gathering) Software installed on Client's dedicated FirstWatch PC/Server
 - FirstWatch to integrate with Client's Motorola PremierOne CAD
 - If needed, 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.
 - FirstWatch to integrate with Client's ImageTrend ePCR and Fire RMS Data Sources via web services interface allowing FirstWatch to securely access, query and receive necessary data via a non-dedicated internet connection, working directly with ImageTrend. Web services interface will include the ability to encrypt and decrypt data and options to query live and historical data. This Software License Agreement between the Client and FirstWatch does not include any potential cost/fees payable to ImageTrend in order for ImageTrend to provide FirstWatch with a full and comprehensive ePCR and RMS data set on behalf of the Client.
 - 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 Client the ability to completely replace each Trigger up to twice per Trigger per year and refinements and adjustments to existing triggers as the Client reasonably requires per any twelve (12) month period during the term.
- 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 – Motorola PremierOne CAD)	1	\$42,464	\$42,464
2	(DS1) Annual Support & Maintenance*	1	\$9,342.08	\$9,342.08
3	(DS1) Installation / Configuration	1	\$2,500	\$2,500
4	(DS1) Data Source Integration	1	\$7,500	\$7,500
5	(DS1) Training / Trigger Consultation	1	\$1,500	\$1,500
6	(DS1) Project Management	1	\$2,500	\$2,500
7	System License* (DS2 – ImageTrend Fire RMS)	1	\$33,972	\$33,972
8	(DS2) Annual Support & Maintenance*	1	\$7,473.84	\$7,473.84
9	(DS2) Data Source Integration	1	\$7,500	\$7,500
10	System License* (DS3 – ImageTrend ePCR)	1	\$33,972	\$33,972
11	(DS3) Annual Support & Maintenance*	1	\$7,473.84	\$7,473.84
12	(DS3) Data Source Integration	1	\$7,500	\$7,500
13	Standard System Triggers (included)	20	Incl.	Incl.
14	Interactive Data Visualization (IDV) Module	1	Incl.	Incl.
15	Online Compliance Utility (OCU) Module	1	\$37,500	\$37,500
16	OCU Annual Support & Maintenance	1	\$8,250	\$8,250
17	OCU – Training / Consulting	1	\$1,500	\$1,500
18	Fire Operations & Accreditation Module (FOAM)	1	\$17,000	\$17,000
19	FOAM Annual Support & Maintenance	1	\$3,740	\$3,740
20	RMS data input into FOAM	1	\$1,500	\$1,500
21	FOAM - Training / Consulting	1	\$740	\$740
			Total Price	\$233,927.76

* License and Maintenance costs are for monitoring Client’s EMS and Fire calls. Assumptions are based on 45,000 annual incidents and include a ‘buffer’ of plus or minus (±) 20% of the call volume.

The City shall pay FirstWatch for work performed, and approved by the City, under this Agreement in accordance with the pricing schedule set forth above.

Maintenance fees beyond the Term of this Agreement 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 5% per year.

Estimated Annual Support & Maintenance for Year 2	\$38,093.75
Estimated Annual Support & Maintenance for Year 3	\$39,998.44
Estimated Annual Support & Maintenance for Year 4	\$41,998.36
Estimated Annual Support & Maintenance for Year 5	\$44,098.26

**Switching Data Sources against “LIVE” OCU and/or FOAM Module(s):
Timing and Financial Considerations**

At least a 90-day notice of a proposed data source change for the FirstWatch OCU and FOAM 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.

***FOAM and Customized Report Development**

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

Contact Information:

Licensor Contact Tax ID No: 05-0544884	Todd Stout, President FirstWatch® 2035 Corte del Nogal, Suite 101 Carlsbad, California 92011	Email : admin@firstwatch.net Phone : 760-943-9123 Fax : 760-942-8329
Client Contact	Steve McKinster, Deputy Fire Chief City of Riverside Fire Department 3401 University Ave Riverside, California 92501	Email : SMcKinster@riversideca.gov Phone : 951-538-3300

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 2019 or Windows 10 Professional including all the latest updates and patches loaded	Microsoft Windows Server 2022 (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.
Client supports remote connections via City operated Vendor Secure Remote Access solution. This access may include standard user access, but elevated user access or administrative access will require IT staff to escort FirstWatch.
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 attended remote access to the dedicated machine via City operated Vendor Secure Remote Access Solution. 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.
This Agreement grants the City of Riverside access to the most current versions of the solution, as they are developed in the future. It also includes vendor certification services for third-party software required by the solution to ensure that no third-party components of the solution will become obsolete during the term of the license. At a minimum, this covers certification for Windows Desktop, Windows Server, Database, middleware, and third-party open source library components of the platform for the duration of the contract. These components will be updated and provided on an annual basis, at the very least. The updates must incorporate all major third-party software releases or long-term support versions that have been released within the past 18 months.

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 City of Riverside Fire Department

This Business Associate Agreement (“Agreement”) between FirstWatch Solutions, Inc. (Business Associate) and City of Riverside Fire Department (Covered Entity) is executed to ensure that Business Associate will appropriately safeguard protected health information (“PHI”) that is created, received, maintained, or transmitted on behalf of Covered Entity in compliance with the applicable provisions of Public Law 104-191 of August 21, 1996, known as the Health Insurance Portability and Accountability Act of 1996, Subtitle F – Administrative Simplification, Sections 261, *et seq.*, as amended (“HIPAA”), and with Public Law 111-5 of February 17, 2009, known as the American Recovery and Reinvestment Act of 2009, Title XII, Subtitle D – Privacy, Sections 13400, *et seq.*, the Health Information Technology and Clinical Health Act, as amended (the “HITECH Act”).

A. General Provisions

1. **Meaning of Terms.** The terms used in this Agreement shall have the same meaning as those terms defined in HIPAA.
2. **Regulatory References.** Any reference in this Agreement to a regulatory section means the section currently in effect or as amended.
3. **Interpretation.** Any ambiguity in this Agreement shall be interpreted to permit compliance with HIPAA.

B. Obligations of Business Associate

Business Associate will:

1. Not use or further disclose PHI other than as permitted or required by this Agreement or as required by law;
2. Use appropriate safeguards and comply, where applicable, with the HIPAA Security Rule with respect to electronic protected health information (“e-PHI”) and implement appropriate physical, technical and administrative safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement;
3. Report to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, including any security incident (as defined in the HIPAA Security Rule) and any breaches of unsecured PHI as required by 45 CFR §164.410. Breaches of unsecured PHI shall be reported to Covered Entity without unreasonable delay but in no case later than 60 days after discovery of the breach;
4. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business

Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information;

5. Make PHI in a designated record set available to Covered Entity and to an individual who has a right of access in a manner that satisfies Covered Entity's obligations to provide access to PHI in accordance with 45 CFR §164.524 within 30 days of a request;
6. Make any amendment(s) to PHI in a designated record set as directed by Covered Entity, or take other measures necessary to satisfy Covered Entity's obligations under 45 CFR §164.526;
7. Maintain and make available information required to provide an accounting of disclosures to Covered Entity or an individual who has a right to an accounting within 60 days and as necessary to satisfy Covered Entity's obligations under 45 CFR §164.528;
8. To the extent that Business Associate is to carry out any of Covered Entity's obligations under the HIPAA Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity when it carries out that obligation;
9. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary of the Department of Health and Human Services for purposes of determining Business Associate's compliance with HIPAA and the HITECH Act;
10. Restrict the use or disclosure of PHI if Covered Entity notifies Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR §164.522; and
11. If Covered Entity is subject to the Red Flags Rule (found at 16 CFR §681.1 *et seq.*), Business Associate agrees to assist Covered Entity in complying with its Red Flags Rule obligations by: (a) implementing policies and procedures to detect relevant Red Flags (as defined under 16 C.F.R. §681.2); (b) taking all steps necessary to comply with the policies and procedures of Covered Entity's Identity Theft Prevention Program; (c) ensuring that any agent or third party who performs services on its behalf in connection with covered accounts of Covered Entity agrees to implement reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft; and (d) alerting Covered Entity of any Red Flag incident (as defined by the Red Flag Rules) of which it becomes aware, the steps it has taken to mitigate any potential harm that may have occurred, and provide a report to Covered Entity of any threat of identity theft as a result of the incident.

C. Permitted Uses and Disclosures by Business Associate

The specific uses and disclosures of PHI that may be made by Business Associate on behalf of Covered Entity include uses or disclosures of PHI as permitted by HIPAA necessary to

perform the services that Business Associate has been engaged to perform on behalf of Covered Entity.

D. Termination

1. Covered Entity may terminate this Agreement if Covered Entity determines that Business Associate has violated a material term of the Agreement.
2. If either party knows of a pattern of activity or practice of the other party that constitutes a material breach or violation of the other party's obligations under this Agreement, that party shall take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful, terminate the Agreement if feasible.
3. Upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity or destroy all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form. Business Associate shall retain no copies of the PHI. If return or destruction is infeasible, the protections of this Agreement will extend to such PHI.

Agreed to this _____ day of _____, 20__.

FirstWatch Solutions, Inc.

City of Riverside Fire Department

Signature: _____

Signature: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

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 support@firstwatch.net