ATTACHMENT D

PROPOSAL FOR FIMS DEVELOPMENT SERVICES ENHANCEMENT



Proposal for FIMS Dev Services Enhancement

October 12, 2022

V1.0

Shakir Shaikh

Director of Applications

601.345.5336

shakir.shaikh@3disystems.com

Submitted by:

3Di, Inc

3 Pointe Drive, STE 307, Brea, CA 92821

Phone: 714.257.1100

Email: marketing@3disystems.com

Web: www.3disystems.com

Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

Document Change Control

Change History

Version	Date	Changes	Author
1.0	10/12/2022	Baselined Version.	Shakir Shaikh

Review Detail

Review #	Date	Name of Reviewer	Signature
1		LAFD team	
2			
3			

Approval Detail

Approval #	Date	Name & Role of Approver	Signature
1			
2			
3			
4			

Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

Table of Contents

1. Project Information **4**

1.1 Goal *4*

1.2 In Scope Use Cases *4*

1.2.1 Tracking Projects 4

1.2.2 Running Reports 4

1.2.3 Assigning Projects 4

1.2.4 Plan Check 4

1.2.5 PCIS 5

1.2.6 Payments 5

1.2.7 Customer Portal 5

1.2.8 Internal Dashboard 5

1.2.9 Other functions 5

2. Project Timeline and Schedule **6**

2.1 Dependency on Migration *6*

2.2 Timeline *6*

2.3 Schedule - Migration *7*

2.4 Schedule – Enhancement *8*

3. Cost **9**

3.1 FIMS 1.0 Operational Cost *9*

3.2 Enhancement Cost *9*

4. Contact **10**

Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

1. Project Information

1.1 Goal

Goal of this project is to enhance the FIMS Dev Services to meet additional functions desired by Staff and LAFD's Customers.

1.2 In Scope Use Cases

1.2.1 Tracking Projects

- Be able to modify/flag projects by certain identifiers
- Find a more effective way to capture the turnaround time on certain projects- e.g. FIMS should be able to quantify the number of days from each step of the plan check process: Date paid to date assigned to date corrections issued to date corrections returned to date plan check approved.
- Automated flagging
- Dashboard and not just reports for managerial use.

1.2.2 Running Reports

- Have ADU, single family dwelling, Mayor's ED30 affordable housing, homeless shelter be their own category instead of having to filter the scope of work field
- Be able to add and change identifiers/flags as needed.
- Be able to run reports for inspection turnaround times for specific flags. E.g. Percentage of inspections within 48 hrs of preferred date inspection requests for specific flagged projects.
- Fire Stat

1.2.3 Assigning Projects

- Be able to assign projects in bulk. Eg. check off transactions in a queue and assign to specific plan checkers/ inspectors.

1.2.4 Plan Check

- Issuing corrections through FIMS
- Create a document management system
- Memory Storage needs
- Auto delete applicant uploaded plans after a certain amount of time
- Be able to add additional fees through FIMS
- Any additional fees and modification are currently done through UCS
- No longer have to use the build LA calendar and have a FIMS appointment system (incorporate BuildLA calendar into FIMS?)
- New workflow for modifications; including, submit and tracking process
- Incorporate plan check OT documents
- Have a fillable expedite form in lieu of the current system of customer uploading the expedite form. When choosing Backroom Expedite, have an electronic signature option

Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

- Time keeping for project review
- Improvements to plan check in progress widget
- Change from "created on" to "Paid on" this allows for easier sorting

1.2.5 PCIS

- Be able to add more than 1 PCIS
- Pull inventory information from PCIS
- Assign PCIS filter

1.2.6 Payments

- Be able to edit transactions when payments are returned
- Currently when payments go through it is recorded in FIMS but when payments are later returned no change can be made to the transaction
- Request and process refunds in FIMS
- Be able to edit transactions that have recorded the customers' payments (receipt number, payment type, and receipt date) yet the status remains Pending Payment and did not update to Pending Assignment
- We usually have to contact 3DI in order to make that change on FIMS which ultimately slows down the turnaround time on some projects
- Integrate the refund request form on FIMS so that customers may submit their request online

1.2.7 Customer Portal

- Pop up notifications/alert when an action is required on their account
- Improve portal workflow

1.2.8 Internal Dashboard

- Be able to toggle between various administrative roles without having to log out and log back in
- Example- Gmail delegated account
- Referral request feature in FIMS between FDS bureaus

1.2.9 Other functions

- Customer request handling
- bot - self learning (chip)
- Pull down menu for assignment hours

Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

2. Project Timeline and Schedule

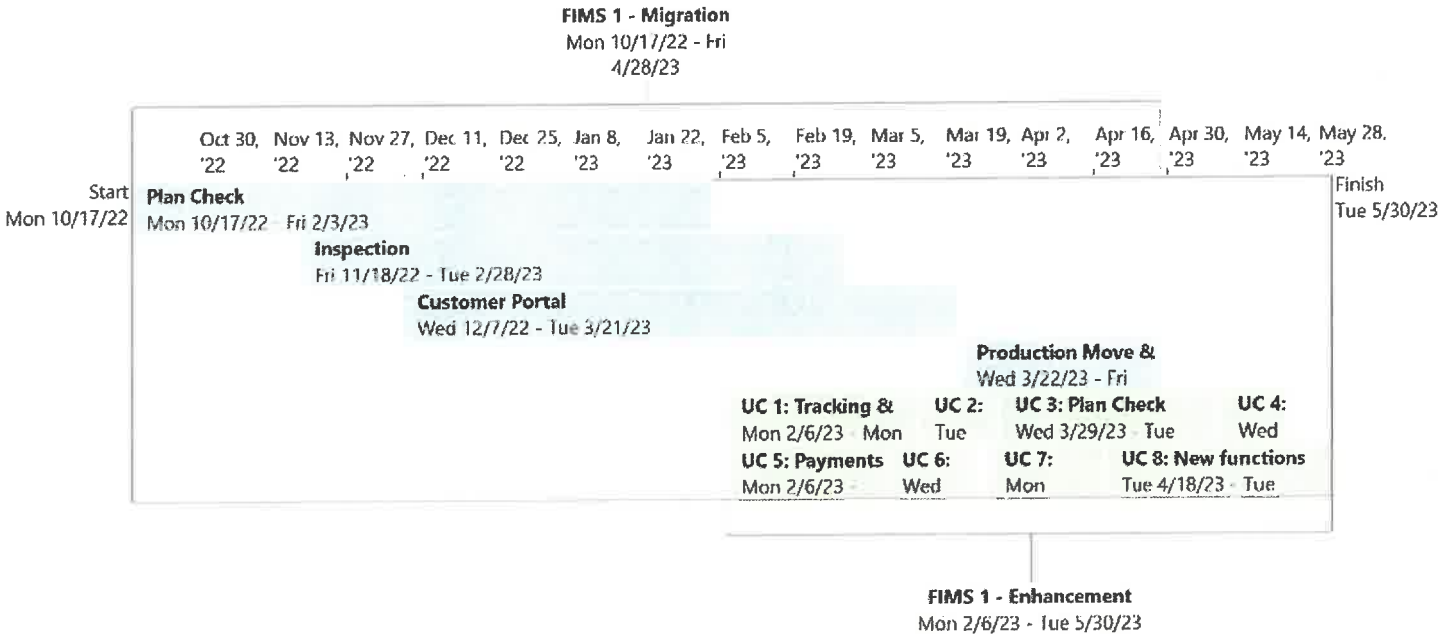
2.1 Dependency on Migration

The current Dev Services solution is running on an old version of technology. Before these enhancements can be implemented, it is important to migrate the Dev Services existing module on FIMS 2.0. As per the original project plan for FIMS 2.0, the Dev Services migration is supposed to start in December 2022. To expedite the enhancements, it's important that migration begins sooner.

The enhancement implementation will start in parallel with the migration. As soon as the Plan Check module UAT is completed, 3Di will begin working on enhancement Use Cases. All the completed enhancement use cases will be available in production along with migration production launch. Remaining will be completed as per the timeline and schedule given below.

2.2 Timeline

Following is the timeline for all the Use Cases along with Migration.



Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

2.3 Schedule - Migration

ID	Task	Duration	Start	Finish	Predecessor
1	**FIMS 1 - Migration**	**127 days**	**Mon 10/17/22**	**Fri 4/28/23**	
2	**Plan Check**	**68 days**	**Mon 10/17/22**	**Fri 2/3/23**	
3	**Kick off & Planning**	**8 days**	**Mon 10/17/22**	**Wed 11/2/22**	
4	Kick Off	1 day	Mon 10/17/22	Mon 10/17/22	
5	Gap analysis & Scope finalization	7 days	Tue 10/18/22	Wed 11/2/22	4
6	**Requirement & Configuration**	**35 days**	**Thu 11/3/22**	**Tue 12/27/22**	**3**
7	Portal Base Setup	10 days	Thu 11/3/22	Thu 11/17/22	
8	Data Analysis for Transfer	5 days	Thu 11/3/22	Wed 11/9/22	
9	Configuration and Testing	15 days	Fri 11/18/22	Mon 12/12/22	7
10	System Testing	10 days	Tue 12/13/22	Tue 12/27/22	9
11	**Validation & Finalization**	**25 days**	**Wed 12/28/22**	**Fri 2/3/23**	**6**
12	User Acceptance Testing	20 days	Wed 12/28/22	Wed 1/25/23	
13	UAT to Production Move	10 days	Thu 1/19/23	Fri 2/3/23	12FF+5 days
14	**Inspection**	**66 days**	**Fri 11/18/22**	**Tue 2/28/23**	**7**
15	**Kick off & Planning**	**6 days**	**Fri 11/18/22**	**Tue 11/29/22**	
16	Kick Off	1 day	Fri 11/18/22	Fri 11/18/22	
17	Gap analysis & Scope finalization	5 days	Mon 11/21/22	Tue 11/29/22	16
18	**Requirement & Configuration**	**35 days**	**Wed 11/30/22**	**Thu 1/19/23**	**15**
19	Base Mobile Setup	5 days	Wed 11/30/22	Tue 12/6/22	
20	Configuration and Testing	20 days	Wed 12/7/22	Wed 1/4/23	19
21	System Testing	10 days	Thu 1/5/23	Thu 1/19/23	20
22	**Validation & Finalization**	**25 days**	**Fri 1/20/23**	**Tue 2/28/23**	**18**
23	User Acceptance Testing	20 days	Fri 1/20/23	Tue 2/21/23	
24	UAT to Production Move	10 days	Tue 2/14/23	Tue 2/28/23	23FF+5 days
25	**Customer Portal**	**70 days**	**Wed 12/7/22**	**Tue 3/21/23**	**19**
26	**Kick off & Planning**	**10 days**	**Wed 12/7/22**	**Tue 12/20/22**	
27	Kick Off	1 day	Wed 12/7/22	Wed 12/7/22	
28	Gap analysis & Scope finalization	9 days	Thu 12/8/22	Tue 12/20/22	27
29	**Requirement & Configuration**	**35 days**	**Wed 12/21/22**	**Mon 2/13/23**	**26**
30	Portal Base Setup	5 days	Wed 12/21/22	Wed 12/28/22	
31	Data Analysis for Transfer	5 days	Wed 12/21/22	Wed 12/28/22	
32	Configuration and Testing	20 days	Thu 12/29/22	Fri 1/27/23	30,31
33	System Testing	10 days	Tue 1/31/23	Mon 2/13/23	32
34	**Validation & Finalization**	**25 days**	**Tue 2/14/23**	**Tue 3/21/23**	**29**
35	User Acceptance Testing	20 days	Tue 2/14/23	Tue 3/14/23	
36	UAT to Production Move	10 days	Wed 3/8/23	Tue 3/21/23	35FF+5 days
37	**Production Move & Go Live**	**28 days**	**Wed 3/22/23**	**Fri 4/28/23**	**25**
38	Data Migration	20 days	Wed 3/22/23	Tue 4/18/23	
39	Production Deployment	5 days	Wed 4/19/23	Tue 4/25/23	38
40	Handover & Support Initiation	3 days	Wed 4/26/23	Fri 4/28/23	39

Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

2.4 Schedule – Enhancement

ID	Task	Duration	Start	Finish	Predecessor
42	**FIMS 1 - Enhancement**	**80 days**	**Mon 2/6/23**	**Tue 5/30/23**	**2**
43	**UC 1: Tracking & Assigning Projects**	**25 days**	**Mon 2/6/23**	**Mon 3/13/23**	
44	Requirement analysis & Scope finalization	3 days	Mon 2/6/23	Wed 2/8/23	
45	Configuration and Testing	7 days	Thu 2/9/23	Fri 2/17/23	44
46	User Acceptance Testing	10 days	Tue 2/21/23	Mon 3/6/23	45
47	UAT to Production Move	5 days	Tue 3/7/23	Mon 3/13/23	46
48	**UC 2: Reports**	**11 days**	**Tue 3/14/23**	**Tue 3/28/23**	**43**
49	Requirement analysis & Scope finalization	1 day	Tue 3/14/23	Tue 3/14/23	
50	Configuration and Testing	3 days	Wed 3/15/23	Fri 3/17/23	49
51	User Acceptance Testing	5 days	Mon 3/20/23	Fri 3/24/23	50
52	UAT to Production Move	2 days	Mon 3/27/23	Tue 3/28/23	51
53	**UC 3: Plan Check**	**30 days**	**Wed 3/29/23**	**Tue 5/9/23**	**48**
54	Requirement analysis & Scope finalization	5 days	Wed 3/29/23	Tue 4/4/23	
55	Configuration and Testing	10 days	Wed 4/5/23	Tue 4/18/23	54
56	User Acceptance Testing	10 days	Wed 4/19/23	Tue 5/2/23	55
57	UAT to Production Move	5 days	Wed 5/3/23	Tue 5/9/23	56
58	**UC 4: PCIS Integration**	**9 days**	**Wed 5/10/23**	**Mon 5/22/23**	**53**
59	Requirement analysis & Scope finalization	1 day	Wed 5/10/23	Wed 5/10/23	
60	Configuration and Testing	3 days	Thu 5/11/23	Mon 5/15/23	59
61	User Acceptance Testing	3 days	Tue 5/16/23	Thu 5/18/23	60
62	UAT to Production Move	2 days	Fri 5/19/23	Mon 5/22/23	61
63	**UC 5: Payments**	**21 days**	**Mon 2/6/23**	**Tue 3/7/23**	
64	Requirement analysis & Scope finalization	3 days	Mon 2/6/23	Wed 2/8/23	
65	Configuration and Testing	5 days	Thu 2/9/23	Wed 2/15/23	64
66	User Acceptance Testing	10 days	Thu 2/16/23	Thu 3/2/23	65
67	UAT to Production Move	3 days	Fri 3/3/23	Tue 3/7/23	66
68	**UC 6: Customer Portal**	**13 days**	**Wed 3/8/23**	**Fri 3/24/23**	**63**
69	Requirement analysis & Scope finalization	2 days	Wed 3/8/23	Thu 3/9/23	
70	Configuration and Testing	3 days	Fri 3/10/23	Tue 3/14/23	69
71	User Acceptance Testing	5 days	Wed 3/15/23	Tue 3/21/23	70
72	UAT to Production Move	3 days	Wed 3/22/23	Fri 3/24/23	71
73	**UC 7: Internal Dashboard**	**16 days**	**Mon 3/27/23**	**Mon 4/17/23**	**68**
74	Requirement analysis & Scope finalization	2 days	Mon 3/27/23	Tue 3/28/23	
75	Configuration and Testing	5 days	Wed 3/29/23	Tue 4/4/23	74
76	User Acceptance Testing	7 days	Wed 4/5/23	Thu 4/13/23	75
77	UAT to Production Move	2 days	Fri 4/14/23	Mon 4/17/23	76
78	**UC 8: New functions**	**30 days**	**Tue 4/18/23**	**Tue 5/30/23**	**73**
79	Requirement analysis & Scope finalization	5 days	Tue 4/18/23	Mon 4/24/23	
80	Configuration and Testing	10 days	Tue 4/25/23	Mon 5/8/23	79
81	User Acceptance Testing	10 days	Tue 5/9/23	Mon 5/22/23	80
82	UAT to Production Move	5 days	Tue 5/23/23	Tue 5/30/23	81

Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

3. Cost

3.1 FIMS 1.0 Operational Cost

FIMS 1.0 current operational cost is $15,000 per month which comprises of 3 modules.

1. Dev Services
2. VMS3
3. R1R2

Until all these modules are migrated over to FIMS 2.0, this cost will continue to prevail. The monthly cost for any module that is migrated over will stop and will be absorbed as part of the FIMS 2.0 subscription cost.

3.2 Enhancement Cost

Following is the cost table for all the enhancement use cases.

Task Name	Duration	Start	Finish	Cost
UC 1: Tracking & Assigning Projects	25 days	Mon 2/6/23	Mon 3/13/23	$48,880.00
UC 2: Reports	11 days	Tue 3/14/23	Tue 3/28/23	$20,680.00
UC 3: Plan Check	30 days	Wed 3/29/23	Tue 5/9/23	$56,400.00
UC 4: PCIS Integration	9 days	Wed 5/10/23	Mon 5/22/23	$16,920.00
UC 5: Payments	21 days	Mon 2/6/23	Tue 3/7/23	$41,360.00
UC 6: Customer Portal	13 days	Wed 3/8/23	Fri 3/24/23	$24,440.00
UC 7: Internal Dashboard	16 days	Mon 3/27/23	Mon 4/17/23	$30,080.00
UC 8: New functions	30 days	Tue 4/18/23	Tue 5/30/23	$58,280.00
Total				**$297,040.00**

Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

4. Contact

Please reach out to Shakir Shaikh (shakir.shaikh@3disystems.com - 601.345.5336) in case you have any further queries.

Copyright © 3Di, 2022. All Rights Reserved. Confidential & Proprietary.

ATTACHMENT E

PROPOSAL FOR CASHIERING SYSTEM

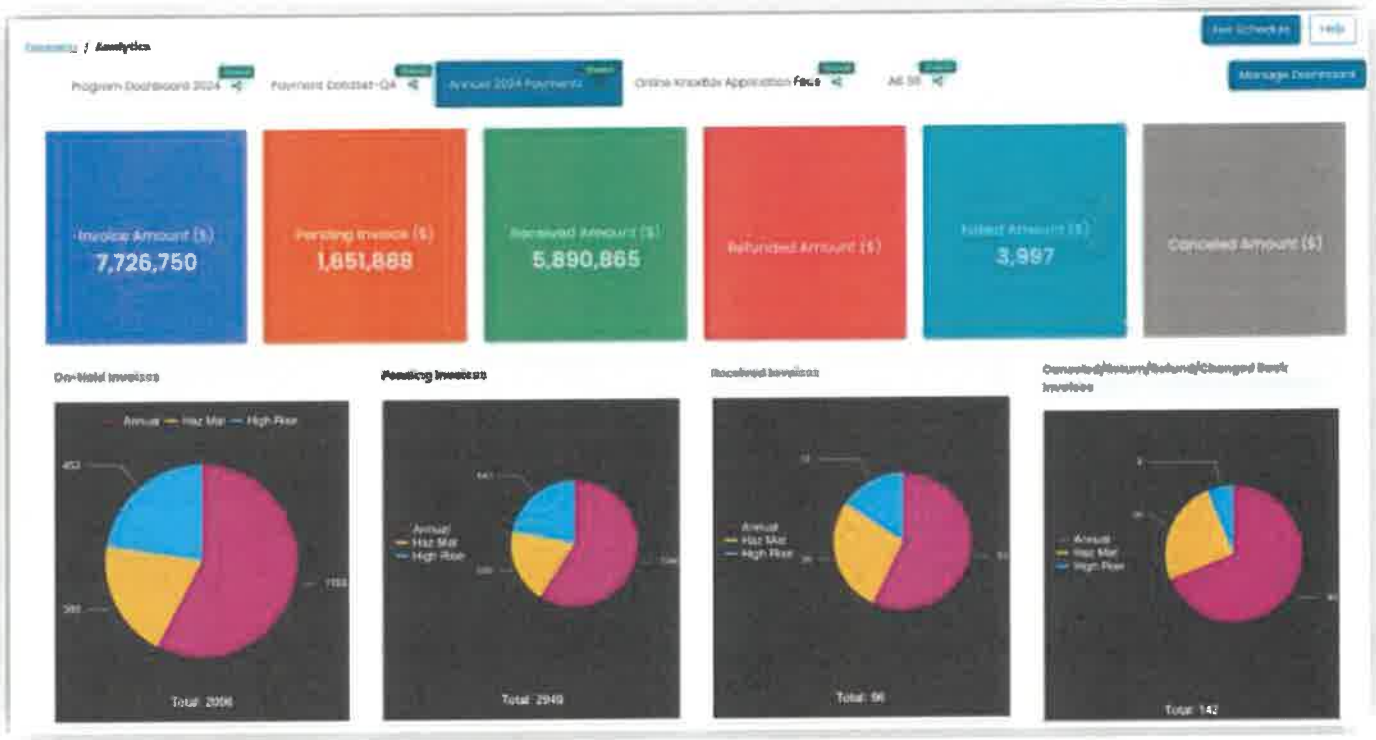
3Di

3Di's proposal for the

Cashiering System

for

Los Angeles Fire Department CTS



Date: 09/25/2025

Submitted by:
3Di, Inc.

Mihir Desai, COO & CFO
3 Pointe Drive, Suite 307
Brea, CA 92821
Office: +1-714-257-1100 Fax: +1-714-257-1386
mihir.desai@3disystems.com

3Di Engage

Copyright © 2025, 3Di.

Table of Content

1 Overview 3

2 Scope 4

3 Proposed Approach 6

4 Schedule & Cost 7

4.1 Schedule 7

4.2 Cost 8

4.3 Pricing Assumptions 8

Copyright © 2025, 3Di

1 Overview

The Los Angeles Fire Department (LAFD) is undertaking a comprehensive modernization of its cashiering and payment processing systems across multiple business units. In partnership with 3Di, this project aims to replace outdated and siloed tools, streamline financial transactions, and enhance service delivery for both internal departments and the public.

This initiative addresses the growing need for centralized, real-time, and user-friendly systems that accommodate the wide range of LAFD services, including permit processing, records management, and subpoena handling. The proposed solution will integrate key functionalities such as Point-of-Sale (POS) support, online payment portals, secure document submission, system interfacing with existing receivables, and advanced reconciliation capabilities.

In alignment with the department's operational and compliance goals, the new system will serve various units including Accounting Services, the Fire Prevention Bureau (FPB), Risk Management, and the EMS Records Unit. The scope includes both enhancements to existing systems such as FIMS 2.0, and the development of new, custom modules for functions not previously automated.

Through this modernization effort, LAFD seeks to achieve:

- Enhanced transparency and tracking of financial transactions across locations
- Reduced reliance on legacy tools (e.g., Access databases)
- Improved customer experience with online services
- Increased security and compliance in the handling of sensitive records

3Di will deliver this solution based on the scope outlined in the section 2, incorporating both existing initiatives and newly identified needs. This proposal outlines each function, its associated requirements, business unit involvement, and the applicable scope classification.

Copyright © 2025, 3Di

2 Scope

	Functions	Requirements/Features	Business Unit	3di Comments
1	**Point of Sale and cashiering for all cash-handling locations**	• Cash, check, advance deposit, credit card for Main Counter CHE 16th floor, Arson, FPB (Valley, Harbor, West), CUPA • Real time viewing, reporting, uploading of documents, and reconciliation for all locations • Timeliness of deposits	Accounting Services Division	New Scope
2	**Fire Receivable System Interface**	• Past due flag - customer receivable clearance certificate process • Payment application back to the receivable system (CUPA, Arson, EMS Records, FMS)	Accounting Services Division	New Scope
3	**Fire Safety Officer and Permitting**	• Replace Access databases - Division 5/Specific Action permit and Public Counter Cash Register • Barcode scanning capability and adding barcodes on internal applications and forms • Permit reconciliations	Accounting Services Division and Fire Prevention Bureau	Permitting is part of FIMS 2.0 already. Barcode and Access DB replacement is New Scope.
4	**Customer Online**	• Customer initiates online FPB FSO or permit application • FPB reviews and approves application • Customer pays online	Accounting Services Division	This is part of FIMS 2.0 scope to create a Customer Portal for FPB permits. The other services and permits can be added as New Scope.
5	**Fire Reports - $5.50**	• Incident Date • Incident Location • Incident number (if available) this should be an optional field • Email address • Phone number "There should be a notice that states that we do not process EMS or traffic accident requests"	Risk Management	New Scope

Copyright © 2025, 3Di

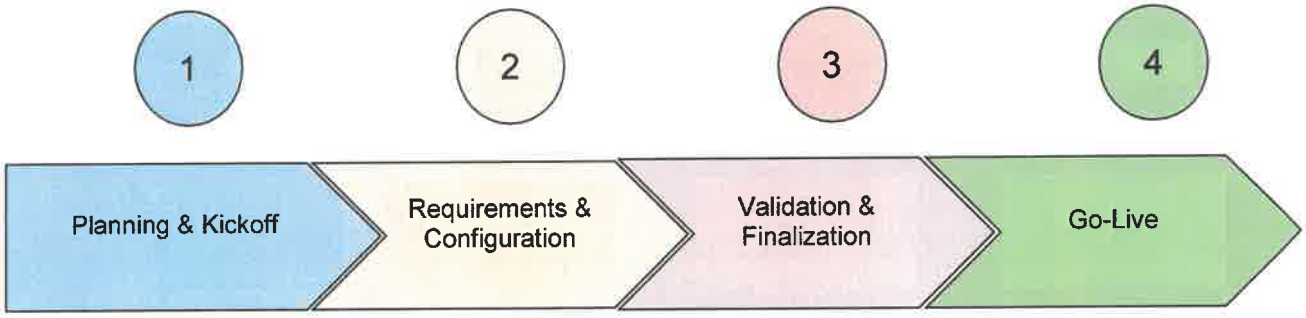
	Functions	Requirements/Features	Business Unit	3di Comments
6	**Subpoenas for "fire" records - $15.00**	• Copy of the subpoena There should be a notice that states that we do not process EMS or traffic accident requests.	Risk Management	New Scope
7	**Subpoena for "personal appearance" - $275.00**	• Name of employee • Date of appearance (must be a minimum of 10 days) • Zoom link if remote (optional) There should be a notice that members do not have access to records and that records should be subpoenaed separately. Can there be an "other" cost section for approved payments for a non-specific amounts such as adding audio ($10.00), photos ($13.00), or approved investigations ($5.50). These items must have approval from lafd.records@lacity.org prior to processing.	Risk Management	New Scope
8	**Subpoena for EMS Records - Initial fee $15**	• Requestor pays Initial Fee • Portal Requires unique keys - WO # and Case # • Requestor Name, Email, Phone # • Portal is connected to Paymentus • Paymentus provides payment receipt • HIPAA secure (encrypted) drop-off for subpoenas	EMS Records Unit	New Scope
9	**Subpoena for EMS Recodrs - Requestor pays Final Balance**	• Portal requires unique keys - WO # and Case # • Portal is connected to Paymentus • Paymentus provides payment receipt	EMS Records Unit	New Scope

Copyright © 2025, 3Di

3 Proposed Approach

3Di will implement the proposed Cashiering and Payment Enhancements as an **additional module** within the existing **FIMS 2.0 (Fire Inspection Management System)** platform. Leveraging the robust foundation already in place—including the base portal architecture, inspection workflows, and customer portal—this approach allows LAFD to maximize existing investments while ensuring seamless integration, consistent user experience, and streamlined system management.

3Di will follow a four-stage implementation methodology outlined below.



Tasks: • Finalize Goals, Scope & Stakeholder Expectations • Identify Project Teams, Roles & Responsibilities • Define Governance Structure & Reporting Requirements • Finalize Project Plan	Tasks: • Requirements & Gap Analysis • App Configuration • Integration (if any) • Testing	Tasks: • System Validation • Use Cases • User Acceptance Testing (UAT) • Training • Go-Live Planning	Tasks: • Go-Live Activities • Hand-Over to Customer • Hand-Over to Support
Milestones: • Kick-Off Meeting • Detailed Project Plan • Scope • Timeline • Resource Allocations • Governance Structure	Milestones: • Requirements Finalized & Signed-Off • Configuration Completed • Integrations Completed • Full System Testing Completed	Milestones: • Validation Completed • UAT Completed • Training Completed • Go-Live Plan Finalized	Milestones: • Go-Live Completed • Hand-Over Completed • Support Initiated

Copyright © 2025, 3Di

4 Schedule & Cost

4.1 Schedule

ID	Task Name	Duration	Start	Finish	Predecessors
1	**Cashiering System**	**51 days**	**Mon 10/6/25**	**Mon 12/29/25**	
2	**Kick off & Planning**	**4 days**	**Mon 10/6/25**	**Thu 10/9/25**	
3	Kick Off	1 day	Mon 10/6/25	Mon 10/6/25	
4	Discovery & Scope Finalization	3 days	Tue 10/7/25	Thu 10/9/25	3
5	**Requirement & Configuration**	**25 days**	**Fri 10/10/25**	**Mon 11/24/25**	**2**
6	**Requirement Analysis**	**15 days**	**Fri 10/10/25**	**Fri 11/7/25**	
7	Accounting Services Division	5 days	Fri 10/10/25	Fri 10/17/25	
8	Risk Management	5 days	Mon 10/27/25	Fri 10/31/25	7
9	EMS Records Unit	5 days	Mon 11/3/25	Fri 11/7/25	8
10	Portal Base Setup	5 days	Fri 10/10/25	Fri 10/17/25	
11	Configuration and Testing	15 days	Mon 11/3/25	Mon 11/24/25	10,6SS+10 days
12	**Validation & Finalization**	**15 days**	**Tue 11/25/25**	**Wed 12/17/25**	**5**
13	User Acceptance Testing	15 days	Tue 11/25/25	Wed 12/17/25	
14	User Training	5 days	Thu 12/11/25	Wed 12/17/25	13FF
15	**Go-Live**	**7 days**	**Thu 12/18/25**	**Mon 12/29/25**	**12**
16	Production Deployment	5 days	Thu 12/18/25	Wed 12/24/25	
17	Handover	2 days	Fri 12/26/25	Mon 12/29/25	16

Copyright © 2025, 3Di

4.2 Cost

	Year 1	Year 2	Year 3	Year 4	Year 5
Section 1: Application Development Services					
Implementaiton Management	$39,680.00				
Requirements Analysis					
Design (includes UX/UI Design) & Discovery					
Development (Build, Configure & Integration)					
System Testing					
Implementation/Deployment					
Post-Implementation Stabilization					
Training					
Total Application Development Services Costs	$39,680.00	$0.00	$0.00	$0.00	$0.00
Section 2: Data Migration (Optional)					
N/A	$0.00				
Total Data Migration Costs	$0.00	$0.00	$0.00	$0.00	$0.00
Section 3: Software Integration (Optional)					
N/A	$0.00				
Total Software Integration Costs	$0.00	$0.00	$0.00	$0.00	$0.00
Section 4: Annual Subscriptions including Ongoing Maintenance, Operations & Support (SaaS)					
Additional Payment Subscription	$12,000.00	$12,360.00	$12,730.80	$13,112.72	$13,506.11
Total SaaS Costs	$12,000.00	$12,360.00	$12,730.80	$13,112.72	$13,506.11
Total Costs	$51,680.00	$12,360.00	$12,730.80	$13,112.72	$13,506.11

4.3 Pricing Assumptions

- 3Di will build this as an additional module on FIMS 2.0.
- The Payment Subscription is discounted based on an active FIMS 2.0 subscription. The price will change if FIMS 2.0 subscription is changed.

Copyright © 2025, 3Di

ATTACHMENT F

PROPOSAL
FOR
MEDICAL RECORDS REQUEST TRACKING SYSTEM

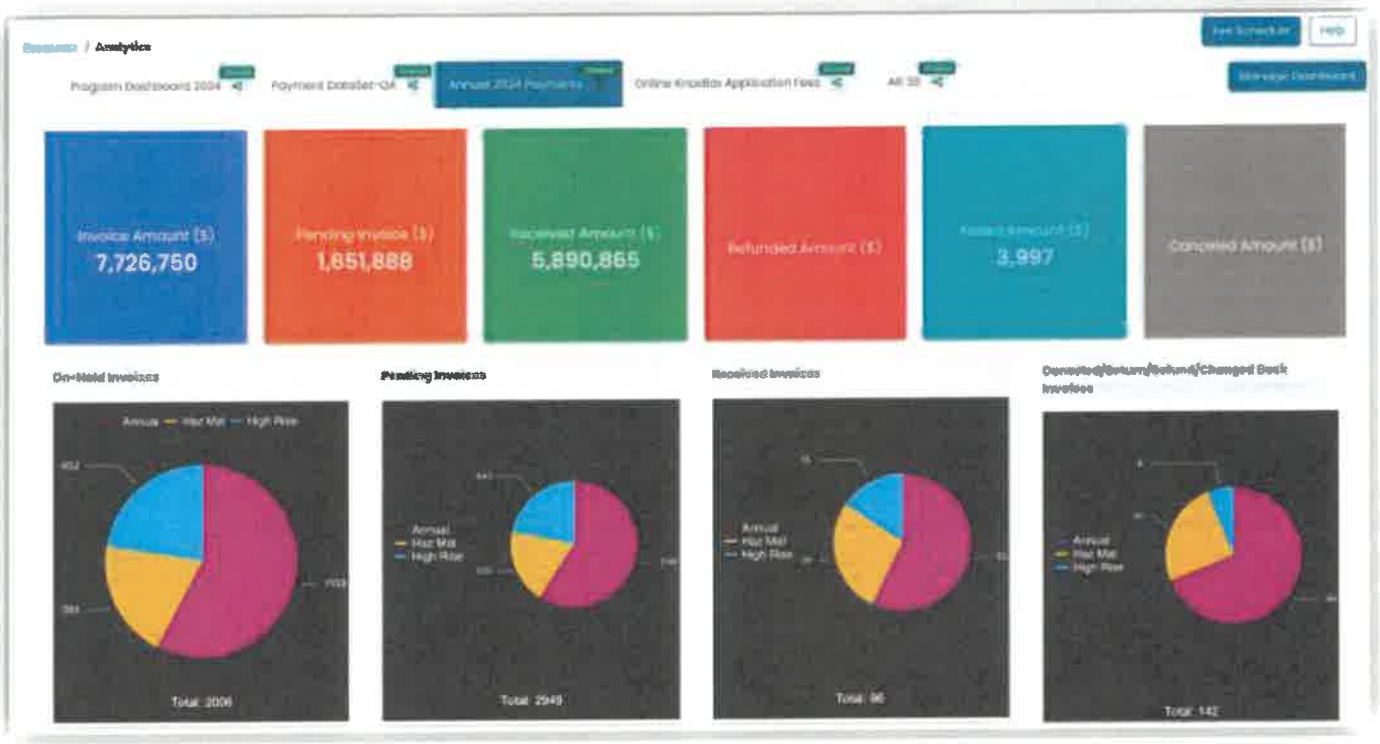
3Di

3Di's proposal for the

Medical Records Request Tracking System

for

EMS Records Unit, Los Angeles Fire Department



Date: 11/26/2025

Submitted by:
3Di, Inc.

Mihir Desai, COO & CFO
3 Pointe Drive, Suite 307
Brea, CA 92821
Office: +1-714-257-1100 Fax: +1-714-257-1386
mihir.desai@3disystems.com

3Di Engage

Copyright © 2025, 3Di.

Table of Content

1 Overview 3

Scope (High-Level System Capabilities) 3

Core Features 3

Estimated Object Counts 3

User Groups 4

Estimated Total Users 4

2 How 3Di will meet MRRTS Requirements 4

3 Innovation Summary 6

Why MRRTS is Innovative 6

Benefits of building MRRTS on Engage (already in use at LAFD): 6

4 Cost 7

4.1 Pricing Assumptions 7

Copyright © 2025, 3Di

1 Overview

The Los Angeles Fire Department's EMS Records Unit handles **10,000+ requests annually** for protected medical information, including patient authorizations, legal subpoenas, law enforcement inquiries, regulatory agency requests, and 9-1-1 audio file releases. These requests currently move through manual, paper-driven steps using an unsupported legacy system (RTS) that is not scalable, not integration-ready, and poses operational and compliance risks.

The proposed **Medical Records Request Tracking System (MRRTS)** will modernize every aspect of this process by providing a **secure, user-friendly, web-based portal** that automates intake, streamlines internal workflow, centralizes communication, ensures compliant PHI release, and provides robust reporting and audit capabilities.

Because LAFD already uses **3Di Engage** for the **FIMS (Fire Inspection/Prevention System)** and the **Cashiering/Payments System**, adopting MRRTS on the same platform ensures **low friction, rapid deployment, interoperability, lower cost, and operational continuity**. The Engage platform is already proven in City environments, compliant with HIPAA security standards, and designed for configurable workflows and secure document handling.

Scope (High-Level System Capabilities)

Core Features

- Public-facing portal for all requestors
- Secure intake forms with dynamic required fields
- eSignature of LAFD release forms
- Identity and document upload (ID, badges, subpoenas, letters)
- Automated unique case ID + tracking
- Staff workflows, task routing, SLAs, escalations
- Secure PHI release via encrypted portal
- Integrated credit-card payments
- Appeals, follow-up communication
- Audit logs and HIPAA-compliant access trails
- Reporting dashboards + ad hoc analytics
- Configurable retention schedules

Estimated Object Counts

- **Cases/Requests per year:** ~10,000+
- **Case Types:**
  - Patient Authorization
  - Subpoena / Process Server
  - Law Enforcement
  - Government / Regulatory Agency
  - Certificate of No Records
  - Appeal/Follow-Up
- **Document Templates:** 10–15 (CNR, declarations, denials, partial releases, subpoenas, etc.)

Copyright © 2025, 3Di

- **Workflow steps:**
  - Intake & Completeness Validation
  - Staff Assignment
  - Task Routing to MFC/OPS/Accounting/City Attorney
  - PHI Collection & Review
  - Secure Release
  - Final Fee Collection
  - Appeals Workflow
  - Closure & Archival

User Groups

- **Public Requestors (~5,000–8,000 unique users/year)**
  Patients, attorneys, law firms, insurance companies, law enforcement, government agencies, process servers
- **LAFD EMS Records Unit (~9 daily users)**
- **Additional Internal Users (~15–25 periodic users)**
  - Supervisors
  - MFC (Audio)
  - EMS Accounting
  - City Attorney staff
  - IT/Ops support

Estimated Total Users

- **External Users:** 5,000–10,000 (self-service portal)
- **Internal Users:** ~25–35

This scale is easily supported by the 3Di Engage platform, which is already handling large volumes for LAHD, LADBS, LAFD Fire Prevention, and other agencies.

2 How 3Di will meet MRRTS Requirements

#	Requirement	FIMS / 3Di Engage Approach
1	**Public-facing request portal** for patients, attorneys, law enforcement, and agencies to submit requests, upload documents, sign forms, and receive PHI.	Engage's configurable **public portal** supports multi-requestor intake, e-signature forms, file uploads, identity verification, request tracking, and secure delivery of PHI. WCAG-compliant.
2	**Unique request ID** creation and status tracking for all requests.	Engage automatically generates a **unique case ID**, supports status visibility, automated notifications, and requestor dashboards.
3	**Role-based assignments** and workflow routing to EMS Records staff, supervisors, MFC, Ops, Accounting, City Attorney, etc.	Engage's workflow engine supports **auto-assignment**, manual assignment, escalations, SLA timers, reminders, and cross-department task routing.

Copyright © 2025, 3Di

#	Requirement	FIMS / 3Di Engage Approach
4	**Completeness review** and secure communication with requestors using templates.	Staff can review submissions, highlight missing items, and send **template-based secure messages** through the portal. Requestors respond via their secure account.
5	**Gathering records from external systems** such as billing, ePCR, dispatch, or audio repositories.	Engage supports **API integrations** with billing, ePCR, CAD/dispatch, and secure file transfers. Manual upload workflow with tagging available if API not available.
6	**Document generation** for Custodian of Records Declaration, CNR, Denial, Partial Denial, and combos.	Engage auto-populates **PDF templates** using merge fields, generating CNRs, declarations, and denial letters automatically.
7	**Secure release of PHI**, encrypted in transit and at rest.	Engage meets HIPAA and CMIA requirements with **AES-256** encryption at rest and **TLS 1.2/1.3** in transit. PHI released via encrypted portal delivery or secure download links.
8	**Payment processing** for subpoena fees and processing fees; routing to Accounting.	Engage integrates with Stripe, Paymentus, PayPal, etc. Automatically logs payments, enforces "no access until paid," and syncs with EMS Accounting.
9	**Appeals, follow-up, and messaging** with full audit logging.	Appeals supported natively. Engage maintains **immutable audit logs** for every access/view, supporting legal compliance and discovery.
10	**Operational, compliance, and financial reporting.**	Engage includes dashboards for volume, SLA compliance, staff workload, backlog, payment history, and ad hoc reporting for analytics and compliance audits.
11	**Retention and archival** aligned with HIPAA & City requirements.	Engage's retention scheduler automatically archives and purges based on configured retention rules.
12	**User and role management** with permissions and MFA.	Engage provides **RBAC**, multi-factor authentication, and granular permissions controlling PHI access.
13	**High security, scalability, and reliability** with HIPAA and BAA requirements.	Engage supports HIPAA, SOC 2-type controls, DR/backup, load balancing, uptime SLAs, and includes a **Business Associate Agreement** with the City.

Copyright © 2025, 3Di

3 Innovation Summary

The proposed MRRTS solution, delivered via FIMS on the 3Di Engage platform, is **not just a replacement** for an outdated system—it represents a **major innovation in how fire departments nationwide manage PHI and records disclosure.** It is a step forward for LAFD and for public-sector EMS agencies across the nation.

Why MRRTS is Innovative

- **No major fire department** currently offers a unified PHI portal supporting all request types (patients, law firms, LEO, process servers, government agencies).
- Existing solutions in the industry (billing portals, ePCR portals) only address fragments of the process — not **subpoenas**, **9-1-1 audio**, **appeals**, **document generation**, **cross-department task routing**, or **integrated fee collection**.
- MRRTS creates a **single digital hub** for intake, validation, communication, secure release, and appeals—something typically only found in high-cost hospital EMR systems.
- It modernizes a legally sensitive, time-critical, high-volume workflow that today relies heavily on PDFs, email, fax, phone calls, paper signatures, and manual tracking.
- Full compliance with **HIPAA, CMIA, PHI encryption**, and audit trails strengthens LAFD's legal position and reduces risk exposure.
- MRRTS will position LAFD as a **national leader and early adopter** of enterprise-grade PHI request management in the fire/EMS sector.

Benefits of building MRRTS on Engage (already in use at LAFD):

- **Shared infrastructure** → reduces cost
- **Shared identity/permissions model** → easier onboarding
- **Shared payment integrations** → quicker setup
- **Consistent UI/UX** → minimal training for staff
- **Existing security/compliance frameworks** → HIPAA-ready
- **Existing SLA, hosting, support processes** → reduces implementation time
- **Proven City of LA deployment track record** → lower risk

Enhancing LAFD's existing Engage ecosystem with MRRTS is the most efficient, scalable, and affordable path. The foundational platform is already operational at LAFD, making MRRTS a natural extension—not a new system—ensuring faster deployment, lower cost, and significantly reduced risk.

Copyright © 2025, 3Di

4 Cost

	Year 1	Year 2	Year 3	Year 4	Year 5
Section 1: Application Development Services					
Implementaiton Management	$48,000.00				
Requirements Analysis					
Design (includes UX/UI Design) & Discovery					
Development (Build, Configure & Integration)					
System Testing					
Implementation/Deployment					
Post-Implementation Stabilization					
Training					
Total Application Development Services Costs	$48,000.00	$0.00	$0.00	$0.00	$0.00
Section 2: Data Migration (Optional)					
N/A	$0.00				
Total Data Migration Costs	$0.00	$0.00	$0.00	$0.00	$0.00
Section 3: Software Integration (Optional)					
N/A	$0.00				
Total Software Integration Costs	$0.00	$0.00	$0.00	$0.00	$0.00
Section 4: Annual Subscriptions including Ongoing Maintenance, Operations & Support (SaaS)					
Additional Payment Subscription	$30,000.00	$30,900.00	$31,827.00	$32,782.00	$33,765.00
Total SaaS Costs	$30,000.00	$30,900.00	$31,827.00	$32,782.00	$33,765.00
Total Costs	$78,000.00	$30,900.00	$31,827.00	$32,782.00	$33,765.00

4.1 Pricing Assumptions

- 3Di will build this as an additional module on FIMS 2.0 platform.
- The Subscription cost is discounted based on an active FIMS 2.0 subscription. The price will change if FIMS 2.0 subscription is changed.

Copyright © 2025, 3Di

ATTACHMENT G

BUSINESS ASSOCIATE AGREEMENT

BUSINESS ASSOCIATE AGREEMENT
BETWEEN
THE CITY OF LOS ANGELES
AND
3Di, INC.

This **Business Associate Agreement** (the "Agreement"), is made as of the 14th day of September, 2026, (the "Effective Date"), by and between 3Di, Inc., on behalf of itself and its subsidiaries and affiliates, (together "Business Associate" or "Business Associates") and the City of Los Angeles ("City"), by and through the Los Angeles Fire Department (the "Covered Entity") and collectively shall be known as the "Parties" in this Agreement. The Agreement is intended to satisfy the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy, security, and breach notification rules promulgated by the U.S. Department of Health and Human Services at 45 C.F.R. Parts 160, 162 and 164, and the Health Information Technology for Economic and Clinical Health Act (hereinafter referred to as "HITECH"), each as amended from time to time (and collectively hereinafter referred to as "HIPAA Rules"), and to ensure compliance with applicable state and local confidentiality and breach notification laws, including and without limitation California law, to the extent not preempted and more stringent than the HIPAA Rules as defined under 45 CFR 160.202.

RECITALS

WHEREAS, Business Associate will perform Services for and on behalf of the Covered Entity involving the processing of Protected Health Information as further described in Annex A (Description of Services) attached hereto and incorporated by reference into this Agreement;

WHEREAS, Covered Entity and Business Associate may have entered into a primary contract (the "Contract") under which Business Associate performs Services involving the creation, receipt, maintenance, or transmission of Protected Health Information on behalf of Covered Entity, or, where no such Contract exists, this Agreement shall govern those Services as a standalone Business Associate Agreement between the Parties;

WHEREAS, the Parties acknowledge that such Protected Health Information is subject to protection under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and their implementing regulations at 45 C.F.R. Parts 160 and 164;

WHEREAS, HIPAA requires that Covered Entity obtain satisfactory assurances that Business Associate will appropriately safeguard Protected Health Information and comply with all applicable privacy, security, and breach notification requirements; and

WHEREAS, the Parties intend this Agreement to satisfy the written-contract requirements set forth in 45 C.F.R. §164.502(e) and §164.504(e), and to ensure that Business Associate provides the same level of protection of Protected Health

Information as is required of Covered Entity under HIPAA and HITECH.

NOW THEREFORE, in consideration of the mutual promises and covenants herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the terms of the Agreement as follows:

A. DEFINITIONS.

Terms not otherwise defined herein shall have the meanings ascribed to them in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), its implementing regulations at 45 C.F.R. Parts 160 and 164, and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), as amended from time to time.

1. Administrative Data

"Administrative Data" means information created, received, or maintained for internal operational, logistical, or support purposes—such as system configurations, scheduling data, staffing records, budgeting materials, or internal communications—that is not used, in whole or in part, to make decisions about an individual and therefore does not form part of the Designated Record Set (DRS) as defined in 45 C.F.R. § 164.501, unless expressly identified otherwise in Annex B (Data Processing Activities). Nothing in this definition shall be construed to remove any information from the scope of Protected Health Information or Business Associate's obligations under this Agreement.

2. Breach

"Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under Subpart E of 45 C.F.R. Part 164, which compromises the security or privacy of such Protected Health Information, subject to the exceptions and exclusions in 45 C.F.R. § 164.402.

3. Business Associate

"Business Associate" or "BA" shall have the meaning given in 45 C.F.R. § 160.103 and refers to [Name of Contractor], its agents, and subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Covered Entity.

4. Contract

"Contract" means Los Angeles City Contract No. C-139201 between the City of Los Angeles (City) and 3Di, Inc., acting as Business Associate, under which the Parties may agree to certain commercial or operational terms. The Contract is separate and distinct from this Agreement and does not modify or limit Business Associate's obligations under this Agreement with respect to Protected Health Information.

5. **Covered Entity (CE)**

"Covered Entity" or "CE" means the Los Angeles Fire Department, a Health Care Component (see "HCC") of the City of Los Angeles, which may operate as a Hybrid Entity as defined in 45 C.F.R. § 164.103 and as defined in this Agreement.

6. **Designated Record Set (DRS)**

"Designated Record Set" means a group of records maintained by or for Covered Entity that are:

(i) medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; and

(iii) other records used, in whole or in part, by or for Covered Entity to make decisions about individuals, as defined in 45 C.F.R. § 164.501.

For purposes of this definition, "record" includes any item or grouping of information containing Protected Health Information that is maintained, collected, used, or disseminated by or for Covered Entity.

7. **De-Identified Information**

"De-Identified Information" means health information that has been de-identified in accordance with 45 C.F.R. § 164.502(d) and the standards and implementation specifications set forth in 45 C.F.R. § 164.514(a)–(b). All documentation supporting de-identification shall comply with the requirements in Section E.4 (De-Identified Information) and any additional specifications in Annex B (Data Processing Activities).

8. **Health Care Component (HCC)**

"Health Care Component" or "HCC" means those portions of a Hybrid Entity that perform covered functions under HIPAA. The LAFD has been designated as a Health Care Component of the City of Los Angeles pursuant to Los Angeles City Council actions (Council File No. 10-1181, July 30, 2010, as modified by Council File No. R3-0240, August 16, 2013).

9. **HIPAA**

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, including all amendments and implementing regulations at 45 C.F.R. Parts 160, 162, and 164.

10. **HITECH Act ("HITECH")**

"HITECH Act" or "HITECH" means the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009, including all implementing regulations, guidance, and compliance dates.

11. **Hybrid Entity**

"Hybrid Entity" means, for purposes of this Agreement, the City of Los Angeles, a single legal municipal entity that performs both HIPAA-covered and non-covered functions and has designated certain components, including the LAFD, as Health Care Components in accordance with 45 C.F.R. § 164.103.

12. **Individual**

"Individual" means the person who is the subject of Protected Health Information, as defined in 45 C.F.R. § 160.103, and includes a Personal Representative authorized under 45 C.F.R. § 164.502(g).

13. **Metadata**

"Metadata" means information that describes, explains, or records the characteristics, structure, context, or management of other data, including but not limited to timestamps, audit trails, geolocation data, device identifiers, user credentials, or system-generated attributes.

Metadata may constitute Protected Health Information if it identifies or could reasonably be used to identify an individual or if it relates to an individual's past, present, or future physical or mental health condition, health care, or payment for care, consistent with 45 C.F.R. § 160.103.

Where metadata forms part of the Designated Record Set (DRS) or is otherwise linked to identifiable Protected Health Information, it shall be treated and safeguarded as Protected Health Information under this Agreement.

14. **Protected Health Information ("PHI")**

"Protected Health Information" or "PHI" has the meaning set forth in 45 C.F.R. § 160.103 and refers to individually identifiable health information transmitted or maintained in any form or medium by or on behalf of the Covered Entity.

15. **Required by Law**

"Required by Law" means a mandate contained in law that compels a use or disclosure of PHI consistent with 45 C.F.R. § 164.512(a).

16. **Security Incident**

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system, including but not limited to breaches of unsecured Protected Health Information, as defined in 45 C.F.R. §164.304 and §164.402. Security Incident does not require include unsuccessful attempts such as pings, port scans, or unsuccessful log-in attempts. All reporting shall follow Annex C (Security Incident and Breach Information Annex).

17. **Secretary**

"Secretary" means the Secretary of the U.S. Department of Health and Human Services (HHS) or their authorized designee.

18. **Subcontractor**

"Subcontractor" means any person or entity to whom Business Associate delegates a function, activity, or Service involving the creation, receipt, maintenance, or transmission of PHI on behalf of Business Associate, as defined in 45 C.F.R. § 160.103.

19. **AI System**

"AI System" means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. AI System-related data activities involving PHI are governed by Annex D (Artificial Intelligence ("AI") System and Automated Processing) Annex.

20. **Services**

"Services" means the activities, deliverables, and functions performed by Business Associates for and on behalf of Covered Entity that involve the creation, receipt, maintenance, processing, or transmission of Protected Health Information, as described in Annex A (Description of Services) and any related data-processing or support activities identified in Annex B (Data Processing Activities).

B. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION IN CONNECTION WITH SERVICES.

In connection with the Services provided by Business Associate to or on behalf of Covered Entity, as described in Annex A (Description of Services), Covered Entity may disclose to Business Associate certain Protected Health Information necessary for Business Associate to perform such Services. Business Associate shall use and disclose Protected Health Information solely for the purposes described in

Annex A and only as permitted by this Agreement, the HIPAA Privacy, Security, and Breach Notification Rules (45 C.F.R. Parts 160 and 164) and applicable law.

Business Associate shall comply with all applicable provisions of HIPAA, the HITECH Act, and their implementing regulations, as amended from time to time, including assuming all responsibilities and liabilities applicable to business associates under 45 C.F.R. Parts 160 and 164, for the duration of this Agreement.

C. RELATIONSHIP OF THE PARTIES; AGENCY.

The parties acknowledge and agree that Business Associate is an independent contractor and **not** an agent, partner, joint venture, or employee of the Covered Entity for purposes of state and municipal law. Nothing in this Agreement shall be construed to create any employment, agency, or fiduciary relationship between the Parties for purposes of state or federal law. Notwithstanding the foregoing, Business Associate recognizes that, exclusively for purposes of HIPAA Privacy and Security Rules and consistent with 45 C.F.R. §160.103 and §164.502(e)(1)(ii), Business Associate, its agents or subcontractors, may be considered to be acting "on behalf of" Covered Entity when performing functions or activities involving Protected Health Information which shall not be construed to alter their independent-contractor status. In such circumstances, Business Associate and its agents or subcontractors shall be subject to all HIPAA obligations and restrictions applicable to Covered Entity with respect to that Protected Health Information. Business Associate shall not represent itself as an agent of Covered Entity in any other context and shall have no authority to bind Covered Entity to any contract, covenant, or obligation except as expressly authorized in writing by Covered Entity. Business Associate shall remain fully responsible for the acts, omissions, and defaults of its agents or subcontractors to the same extent as if such acts or omissions were those of Business Associate itself.

D. RIGHTS AND OBLIGATIONS OF COVERED ENTITY.

1. Notice of Privacy Practices.

   Covered Entity shall notify Business Associate, in writing and without unreasonable delay, of any limitation in Covered Entity's Notice of Privacy Practices (45 C.F.R. §164.520) that may affect Business Associate's permitted uses or disclosures of Protected Health Information.

2. Individual Authorization.

   Covered Entity shall promptly inform Business Associate of any change in, or revocation of, an individual's authorization to use or disclose Protected Health Information, to the extent such change affects Business Associate's permitted activities.

3. Restriction on Use or Disclosure.

Covered Entity shall notify Business Associate of any restriction on the use or disclosure of Protected Health Information agreed to by Covered Entity under 45 C.F.R. §164.522, to the extent that such restriction may affect Business Associate's use or disclosure.

4. Permissible Requests.

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would be impermissible under HIPAA, the HITECH Act, and their implementing regulations, including 45 C.F.R. §164.504(e)(2)(i).

5. Determination of Suspected or Confirmed Incident or Breach and Information Cooperation.

Covered Entity shall make the final determination as to whether any reported use or disclosure of Protected Health Information by Business Associate constitutes an incident or a suspected or confirmed breach of unsecured Protected Health Information within the meaning of 45 C.F.R. §164.402 and shall determine the need for notification under 45 C.F.R. §164.404, §164.406 and §164.408. Business Associate shall, upon Covered Entity's request, provide all information necessary for Covered Entity to make such determination, including, but not limited to:

- a description of the incident, suspected or confirmed breach and the discovery timeline;
- the categories and approximate volume of Protected Health Information involved;
- mitigation and containment steps taken; and
- copies of any forensic, investigative, or incident-response reports.

All suspected or confirmed incident or breach details and supporting documentation shall be submitted in accordance with Annex C (Security Incident and Breach Information Annex), which is incorporated herein by reference and forms an integral part of this Agreement. Business Associate shall provide this information without unreasonable delay and in no event later than five (5) business days following Covered Entity's written request. Business Associate shall continue to supplement the information as new facts become known.

6. Covered Entity Rights.

Covered Entity reserves the right to monitor Business Associate's compliance with this Agreement, to request evidence of safeguards, to audit relevant records, to require remediation of identified discrepancies, or to

require additional documentation to support Covered Entity's analysis for regulatory reporting.

E. OBLIGATIONS OF BUSINESS ASSOCIATE.

Business Associate's obligations under this section are in addition to, and not in limitation of, Business Associate's notification under 45 C.F.R. §164.410 (Notification by a Business Associate).

Business Associate agrees to comply with applicable federal and state privacy and security laws, specifically the provisions of the HIPAA Administrative Simplification to the extent applicable to business associates. Business Associate shall ensure that these obligations are included in all downstream agreements in accordance with 45 C.F.R. 164.504(e)(2)(ii)(D).

1. Use and Disclosure of Protected Health Information.

Business Associate shall use or disclose Protected Health Information only as necessary to perform the Services described in Annex A (Description of Services), or as Required by Law, and only to the extent such use or disclosure is permitted by this Agreement and the HIPAA privacy and security rules (45 CFR Parts 160 and 164).

Business Associate shall not use or disclose Protected Health Information in any manner that would be impermissible if done by the Covered Entity, and shall implement appropriate administrative, physical, and technical safeguards to prevent such use or disclosure as required by 45 C.F.R. §164.504(e)(2)(ii)(B).

Without limiting the foregoing, Business Associate agrees that it shall not:

(a) Use Protected Health Information for marketing, product development, profiling, or any commercial purpose other than as authorized in writing by Covered Entity, in accordance with 45 C.F.R. §164.502(a)(5)(ii);

(b) Sell, externally disclose, put in secondary use, or de-identify, unless de-identification complies with §45 C.F.R. 164.514, Protected Health Information without express written authorization by Covered Entity's legal counsel or an administrative representative;

(c) Use Protected Health Information for machine learning, artificial intelligence training, algorithmic modeling, or similar automated processing activities or purposes except as expressly authorized in writing by Covered Entity's legal counsel or an administrative representative and in accordance with Annex D (Artificial Intelligence (System) and Automated Processing), which is incorporated herein by reference; and

(d) Disclose Protected Health Information to any third party other than as necessary to perform the Services under this Agreement (and as summarized in Annex A) and only after obtaining written assurances that such third party will (i) maintain confidentiality and security of Protected Health Information in accordance with this Agreement and the HIPAA Rules, and (ii) report to Business Associate, without unreasonable delay after discovery, any actual or suspected breach of unsecured Protected Health Information, unauthorized use or disclosure of Protected Health Information, or Security Incident so that Business Associate can meet its own notification and mitigation obligations under the HIPAA Breach Notification Rules (45 C.F.R. §§164-400-414) and this Agreement.

(e) Use Protected Health Information for any a purpose other than its own proper management and administration of Protected Health Information or to carry out its legal responsibilities only to the extent permitted by 45 C.F.R. §164.504(e)(4), and only if Business Associate obtains reasonable assurances that any recipients will maintain Protected Health Information confidentially and notify Business Associate of any breach or violation as set forth in this Section.

2. Suspected or Confirmed Security Incident or Breach Notification.

(a) Prompt Notice of Impermissible Use or Disclosure. Business Associate shall report to the Covered Entity any suspected or confirmed Security Incident or Breach of unsecured Protected Health Information without unreasonable delay and no later than seventy-two (72) hours after discovery, as defined in 45 C.F.R. §164.402.

Business Associate's report shall be submitted in accordance with Annex C (Security Incident and Breach Information Annex) and shall include, at a minimum, the information described therein. Business Associate shall supplement its report promptly as additional facts become known and shall cooperate fully with Covered Entity's investigation and mitigation activities. Covered Entity retains sole authority to determine whether any incident constitutes a reportable breach under 45 C.F.R. §164.402, applying the four-factor risk assessment criteria in §164.402(2)(i)-(iv), and whether notification under §164.404-410 are required.

(b) Cooperation and Determination Breach. Business Associate acknowledges that Covered Entity is solely responsible for determining whether a reportable "breach" of unsecured Protected Health Information has occurred within the meaning of 45 C.F.R. §164.402 and for performing all required notifications under §§164.404, 164.406, and 164.408. Business Associate shall cooperate fully with Covered Entity's investigation, provide requested documentation, and implement reasonable mitigation measures

at Business Associate's sole cost.

(c) Compliance with 45 C.F.R. §164.410 – Notification by a business associate. Business Associate shall comply with the breach-notification obligations applicable to business associates under 45 C.F.R. §164.410, including providing notification of a discovered breach no later than sixty (60) calendar days and maintaining written policies and records of all breach-related activities for at least six (6) years as required by §164.530(j)(2). Nothing in this subsection shall be interpreted to require Business Associate to provide notice directly to individuals or regulators unless Covered Entity directs otherwise in writing.

(d) Relationship Reminder. Business Associate performs the Services as an independent contractor to Covered Entity. The Parties' relationship is governed by Section C "Relationship of the Parties; Agency" clause. This paragraph is included for reference only and does not alter that relationship.

3. Data Aggregation.

(a) Limitation on Use.

Business Associate shall not use or disclose Protected Health Information for data aggregation, analytics, benchmarking, or any other combined-dataset activity involving Protected Health Information received from multiple Covered Entities, unless expressly authorized in advance and in writing by Covered Entity in accordance with 45 C.F.R. § 164.504(e)(2)(i)(B).

(b) Authorized Aggregation.

If Covered Entity provides written authorization for data aggregation, such use shall be limited exclusively to health-care operations, payment, or quality-improvement activities permitted under 45 C.F.R. § 164.506(c) and § 164.501, and shall remain subject to all applicable restrictions of this Agreement, including data-minimization, role-based access, and safeguard requirements under 45 C.F.R. §§ 164.308, 164.310, and 164.312.

(c) Prohibition on Secondary Use.

Business Associate shall not:

1. Combine or compare Covered Entity's Protected Health Information with Protected Health Information received from any other Covered Entity or client for marketing, product development, AI training, or other non-authorized purposes;

2. De-identify Covered Entity's Protected Health Information for independent commercial use under 45 C.F.R. § 164.514(b) without Covered Entity's prior written consent; or
3. Claim, assert or acquire any ownership, license, proprietary, or derivative rights in any aggregated or De-Identified Information created from or derived from Covered Entity's Protected Health Information, nor shall Business Associate use such information for any secondary, commercial, analytical, or model development purpose not covered in this Section and without Covered Entity's prior written authorization.

(d) Safeguards and Reporting.

Business Associate shall maintain segregated environments for Protected Health Information from each Covered Entity, implement technical and administrative controls to prevent cross-contamination of datasets, and promptly notify Covered Entity of any unauthorized aggregation, analysis, or commingling of Covered Entity's Protected Health Information.

(e) Ownership and Control.

All Protected Health Information, whether individually or as part of an aggregated dataset, remains the sole property and in control of Covered Entity. Business Associate acquires no rights in Protected Health Information other than those necessary to perform Services and for duration of term of this Agreement. Any aggregated information created under Covered Entity's written authorization shall be deemed Covered Entity's confidential information and subject to the same protections as Protected Health Information under this Agreement.

4. De-identified Information.

(a) Business Associate may create, use, or disclose de-identified health information only if:

1. Written Authorization. Such use or disclosure is fully disclosed to and expressly authorized in writing by the Covered Entity, which may grant or withhold authorization in its sole discretion;
2. Regulatory Compliance. The de-identification is performed in strict compliance with 45 C.F.R. § 164.502(d) and meets the standards and implementation specifications for de-identification under 45 C.F.R. § 164.514(a) and (b); and
3. Methodology Disclosure. Business Associate shall document the de-identification process used, including whether the Expert Determination or Safe Harbor method was applied, and shall provide Covered Entity with a written summary of the techniques, tools, or

statistical methods used to achieve de-identification, as required under § 164.514(b).

4. Limitations on Use. Business Associate shall not use or disclose any de-identified information for secondary or commercial purposes (including data analytics, AI model training, or research) without Covered Entity's prior written approval and shall not attempt or permit any re-identification of such information.

5. Safeguards.

Business Associate shall maintain appropriate safeguards to ensure that Protected Health Information is not used or disclosed other than as permitted by this Agreement or as Required by Law. Business Associate shall implement the administrative, physical, and technical safeguards required by 45 C.F.R. §§ 164.308, 164.310, and 164.312, as applicable, to reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic PHI ("ePHI") that it creates, receives, maintains, or transmits on behalf of Covered Entity.

Such safeguards shall include, at a minimum:

- Encryption of ePHI at rest and in transit consistent with NIST FIPS 140-2 validated cryptographic standards;
- Maintenance of written policies and procedures for access control, audit logging, user authentication, and system monitoring; and
- Integration of incident response and breach notification coordination with Covered Entity in accordance with Section E.13 (Incident Response).

Business Associate shall, on an annual basis or upon reasonable request, provide Covered Entity with (i) a copy or executive summary of its most recent security risk analysis conducted pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(A), and (ii) its corresponding risk management or remediation plan addressing identified vulnerabilities.

6. Minimum Necessary.

Business Associate shall ensure that all uses, disclosures, and requests for Protected Health Information are limited to the minimum necessary to accomplish the intended purpose, in accordance with 45 C.F.R. § 164.514(d).

To operationalize this requirement, Business Associate shall:

- Implement role-based access controls (RBAC) limiting access to Protected Health Information solely to personnel whose job functions require such access, as documented in written access control matrices;
- Establish tiered access permissions that differentiate between classes of users (e.g., billing, customer support, technical operations) to prevent overexposure of Protected Health Information;
- Periodically review and validate user access rights (at least annually or upon role changes) to ensure compliance with the minimum necessary standard; and
- Configure systems to limit query, view, and export functions to the minimum data elements necessary for each authorized task or transaction.

Business Associate shall document and make available to Covered Entity, upon reasonable request, its policies and procedures demonstrating adherence to this principle and the technical and administrative controls used to enforce it.

7. Disclosure to Agents and Subcontractors.

If Business Associate discloses Protected Health Information to any agent or subcontractor, Business Associate shall require that such agent or subcontractor agree in writing to the same restrictions, conditions, and safeguards that apply to Business Associate under this Agreement and in compliance with 45 C.F.R. § 164.502(e) and § 164.308(b).

Business Associate shall:

- Disclose in writing to Covered Entity all subcontractors that will create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate;
- Maintain and, upon request, provide Covered Entity with a current list of all subcontractors or agents that handle Protected Health Information;
- Ensure each subcontractor implements reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of Protected Health Information; and
- Make such subcontractors available for audit or inspection by Covered Entity upon reasonable notice.

Business Associate shall remain fully liable for any acts, omissions, or failures of its agents or subcontractors as if they were Business Associate's own.

8. Individual Rights Regarding Designated Record Sets.

If Business Associate maintains a Designated Record Set on behalf of Covered Entity, it shall support Covered Entity in fulfilling individuals' rights of access under 45 C.F.R. § 164.524 as follows:

(a) Access and Copies of Protected Health Information.

If Business Associate receives a direct request from an individual for access to or a copy of their Protected Health Information, Business Associate shall forward such request to Covered Entity within ten (10) calendar days of receipt to allow Covered Entity to comply with the 30-day response period under 45 C.F.R. § 164.524(b)(2).

Business Associate shall promptly assist Covered Entity in providing access in the requested form or format, if readily producible, or in an agreed-upon summary format, and shall provide all relevant Protected Health Information necessary for Covered Entity's timely response.

Any reasonable, cost-based fees shall be administered in accordance with Covered Entity's established HIPAA policies.

(b) Amendment of Protected Health Information.

If Business Associate maintains Protected Health Information in a Designated Record Set, Business Associate shall make such records available to Covered Entity for amendment in accordance with 45 C.F.R. § 164.526.

Upon receipt of a request for amendment, Business Associate shall notify Covered Entity within ten (10) calendar days and implement any approved amendment or link to the amendment statement as directed by Covered Entity.

(c) Accounting of Disclosures.

Business Associate shall maintain documentation of disclosures of Protected Health Information sufficient to enable Covered Entity to provide an accounting of disclosures under 45 C.F.R. § 164.528, including the date, purpose, and recipient of each disclosure not otherwise exempt.

Business Associate shall provide such documentation to Covered Entity within ten (10) calendar days of Covered Entity's request to allow Covered Entity to meet the 60-day response period required by the HIPAA Rule.

The accounting shall cover disclosures made in the six (6) years preceding the request (excluding those prior to the HIPAA compliance date).

The first accounting requested by an individual within any twelve-month period shall be provided at no cost; subsequent requests may incur a reasonable, cost-based fee, provided Covered Entity is notified in advance and given an opportunity to withdraw or modify the request.

(d) Cooperation and Documentation.

Business Associate shall maintain and make available to Covered Entity, upon request, all policies, logs, and procedures used to comply with this Section 8 and shall cooperate fully to ensure Covered Entity's timely and compliant response to individual rights requests.

9. Internal Practices, Policies and Procedures.

Except as otherwise specified herein, Business Associate shall make available its internal practices, policies and procedures relating to the use and disclosure of Protected Health Information, received from or on behalf of Covered Entity to the Secretary or his or her agents for the purpose of determining Covered Entity's compliance with the HIPAA Rules, or any other health oversight agency, or to Covered Entity. Records requested that are not protected by an applicable legal privilege will be made available in the time and manner specified by Covered Entity or the Secretary.

10. Notice of Privacy Practices.

Business Associate shall comply with the limitations set forth in Covered Entity's current Notice of Privacy Practices ("NPP"). Any changes to the NPP that affect Business Associate's permitted uses or disclosures of Protected Health Information shall apply only after Business Associate receives written notice of such changes. Uses or disclosures made in good-faith reliance on a prior NPP before receipt of the amended notice shall not constitute a breach of this Agreement.

11. Withdrawal of Authorization.

If Business Associate's use or disclosure of Protected Health Information is based on an Individual's authorization and Business Associate receives notice that such authorization has been revoked, has expired, or is otherwise invalid, Business Associate shall immediately cease all use and disclosure of the affected Protected Health Information, except to the extent

such actions were taken in good-faith reliance on a valid authorization prior to notice, or where an express HIPAA exception applies.

12. Knowledge of HIPAA Rules.

Business Associate agrees to review and understand the HIPAA Rules as it applies to Business Associate, and to comply with the applicable requirements of the HIPAA Rule, as well as any applicable amendments.

13. Security Incident.

(a) Definition and Distinction.

For purposes of this Agreement:

- A "Security Incident" has the meaning set forth in 45 C.F.R. § 164.304 — the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations, involving electronic Protected Health Information.
- A "Breach" has the meaning set forth in 45 C.F.R. § 164.402, as reflected in the Definitions section of this Agreement, and triggers the notification obligations under 45 C.F.R. § 164.410.

(b) Incident Response Procedures.

Business Associate shall maintain and follow written incident detection, response, and documentation procedures designed to identify, contain, and remediate Security Incidents involving Protected Health Information or ePHI.

(c) Reporting Obligations.

1. Business Associate shall report any suspected or confirmed Security Incident to Covered Entity without unreasonable delay and no later than seventy-two (72) hours after discovery.
2. The initial notice shall include, to the extent known:

   (i) the nature and scope of the incident;

   (ii) the date and time of discovery;

   (iii) systems and data elements involved;

   (iv) estimated volume of records affected;

(v) containment and mitigation measures taken; and

(vi) contact information for Business Associate's incident lead.

3. Business Associate shall provide a follow-up written report within five (5) business days containing a root cause analysis, corrective action plan, and evidence of containment and recovery activities.

(d) Cooperation and Preservation.

Business Associate shall:

- Cooperate fully with Covered Entity, its designees, and law enforcement in any investigation or mitigation efforts;
- Preserve all relevant logs, records, and evidence for a minimum of six (6) years from the date of discovery; and
- Refrain from making public statements regarding the incident without Covered Entity's prior written approval.

(e) Breach Notification.

If Business Associate determines that a Security Incident constitutes a Breach of Unsecured Protected Health Information under 45 C.F.R. § 164.410, Business Associate shall provide Covered Entity with a written breach notification meeting the content and timing requirements of the HIPAA Breach Notification Rule.

(f) Continuous Improvement.

Following any incident or breach, Business Associate shall update its incident response plan and implement appropriate corrective and preventive measures to reduce the likelihood of recurrence and shall provide Covered Entity with documentation of such actions upon request.

F. TERM AND TERMINATION

1. Term.

The Term of this Agreement shall be effective as of the Effective Date of the Contract, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

2. Termination for Cause.

Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(a) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and the Contract if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(b) Immediately terminate this Agreement and the Contract if Business Associate has breached a material term of this Agreement and cure is not possible; or

(c) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

3. Effect of Termination.

(a) Return or Destruction of Protected Health Information.

Upon termination or expiration of this Agreement, for any reason, Business Associate shall immediately cease all use and disclosure of Protected Health Information received from, or created or maintained on behalf of, Covered Entity. Unless otherwise agreed based on technical feasibility, Business Associate shall, within thirty (30) days, return or securely destroy all such Protected Health Information, including all copies, extracts, or derivative data, in any form or medium, whether maintained by Business Associate or any of its agents or subcontractors.

Business Associate shall confirm completion of return or destruction to Covered Entity in writing, specifying:

- The date and method of destruction or return;
- The type and volume of Protected Health Information destroyed or returned; and
- The authorized individual who supervised the process.

No copies of Protected Health Information shall be retained by Business Associate, its agents or subcontractors, except as expressly provided in subsection (b).

(b) Infeasibility of Return or Destruction.

If Business Associate determines that return or destruction of Protected Health Information is infeasible, Business Associate shall, within ten (10)

days of such determination, provide Covered Entity with written notice describing:

- The specific reasons why return or destruction is infeasible (e.g., legal retention obligations, backup dependencies, active litigation holds); and
- The approximate duration and scope of such infeasibility.

Upon Covered Entity's approval, Business Associate shall:

- Continue to safeguard the Protected Health Information in accordance with this Agreement and 45 C.F.R. Parts 160 and 164;
- Limit further use and disclosure to those purposes that make return or destruction infeasible; and
- Apply the same administrative, physical, and technical safeguards required under this Agreement until Protected Health Information is returned or destroyed.

(c) Bankruptcy and Cessation of Operations.

In the event Business Associate becomes insolvent, declares bankruptcy, ceases operations, or is otherwise unable to perform its obligations under this Agreement, Business Associate (or its lawful successor, trustee, or receiver) shall:

- Immediately notify Covered Entity of such event; and
- Return or securely destroy all Protected Health Information in its possession, custody, or control prior to or concurrent with cessation of operations.

No Protected Health Information may be treated as a bankruptcy estate asset, and title to all Protected Health Information remains vested exclusively in Covered Entity.

(d) Audit and Certification.

Upon Covered Entity's request, Business Associate shall certify in writing that it and its agents or subcontractors have complied with this Section, and Covered Entity may, at its discretion, audit or inspect Business Associate's destruction or return records to verify compliance.

Business Associate's obligations under this Section, including the duty to safeguard Protected Health Information and to limit its use and disclosure, shall survive termination of this Agreement for as long as Business Associate retains Protected Health Information.

G. LIABILITY, INDEMNIFICATION, MITIGATION, AND PROPRIETARY

RIGHTS

1. Indemnification

(a) Regulatory Proceedings and Compliance Costs. For avoidance of doubt, the indemnification obligations under this Section expressly include all regulatory, administrative, and compliance-related costs that the Covered Entity reasonably incurs as a result of, or in connection with, any breach, Security Incident, or violation by Business Associates, its agents or subcontractor and excludes penalties to the extent not insurable or prohibited by law. Such indemnification amounts include, without limitation:

(i) Costs of responding to investigations, audits, inquiries, or enforcement actions by the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), or any other federal or state authority;

(ii) Cost of implementing or monitoring any Corrective Action Plan (CAP), resolution agreement, or consent order imposed by OCR or any other regulatory body;

(iii) Attorneys' fees, expert, consulting, and forensic expenses incurred in responding to or defending such proceedings; and

(iv) Reasonable internal personnel costs and outside-vendor expenses associated with compliance reviews, risk analysis, documentation, and policy revisions that OCR or other regulatory require.

These costs are recoverable to the fullest extent permitted by 45 C.F.R. Part 160, Subpart D (Enforcement Rule) and applicable law, and are deemed first-party losses for purposes of indemnification and insurance coverage under this Agreement.

(b) To the extent permitted by law, Business Associate shall indemnify and hold harmless Covered Entity from and against all claims, demands, liabilities, losses, costs, fines, penalties, judgments or causes of action of any nature for any relief, elements of recovery or damages recognized by law (including, without limitation, reasonable attorney's fees, defense costs, expert/forensic costs and equitable relief), for any damage or loss incurred by Covered Entity arising out of, resulting from, or attributable to:(i) Business Associate or its agent(s)/sub-contractor(s) breach of this Agreement; (ii) any violation of HIPAA, HITECH, or other applicable privacy or cybersecurity law by Business Associate, its agents or subcontractor; any security incident or breach of unsecured PROTECTED HEALTH INFORMATION (as defined in 45 CFR 164.402), attributable to acts or omissions of Business Associate, its agents/ or subcontractor; and (iv) any failure to comply with 45 CFR §§164.308-312 or §164.504(e). This indemnity shall not be construed to limit Covered Entity's rights, if any, to common law indemnity.

(c) First-Party Costs. Indemnified amounts include first-party costs reasonably incurred by the Covered Entity in responding to a Security Incident or Breach, including: investigation and forensics; containment and eradication; data restoration; legally required and Covered Entity-directed notifications; call-center services; credit monitoring/identity theft protection; mailing and printing; public relations/crisis communications; regulatory inquiries, audits, and OCR resolution/CAP implementation; and reasonable attorney's fees.

(d) Tender and Control of Defense. Upon written notice by Covered Entity of a claim subject to indemnity, Business Associate shall promptly assume the defense using counsel reasonably acceptable to Covered Entity. Covered Entity may participate at its own expense, provided however, if Covered Entity reasonably determines that a conflict of interest prevents joint representation, Business Associate shall fund separate counsel for Covered Entity that is reasonably acceptable to Business Associate. Business Associate shall not settle any claim without Covered Entity's prior written consent if the settlement: (1) imposes any non-monetary obligation on Covered Entity; (2) admits fault by Covered Entity; or (3) fails to unconditionally release Covered Entity. Covered Entity may elect to retain control of the defense with counsel of its choosing. In such event, Business Associate shall reimburse Covered Entity's reasonable defense costs for claims subject to indemnity.

(e) Subcontractor(s) and Agent(s) of Business Associate. Business Associate's obligations extend to acts and omissions of its agents or subcontractors and agent(s) to the same extent as Business Associate's own acts and omissions. Business Associate shall not assert lack of privity as a defense.

(f) No Limitation/Caps for Certain Claims. No limitation of liability (contractual or otherwise) shall apply to Business Associate's obligations under this Agreement with respect to: (i) Breach of Unsecured PROTECTED HEALTH INFORMATION or Security Incident; (ii) violation of confidentiality obligations; (iii) infringement/misappropriation of Covered Entity's IP or data; or (iv) Business Associate's gross negligence, fraud, or willful misconduct.

(g) Savings Clause. The indemnity in this Agreement shall be enforced to the maximum extent permitted by applicable law. If any portion is held invalid, the remaining provisions shall continue in full force.

2. Set-off and Survival.

All obligations of the Parties under this Agreement, including indemnification, confidentiality, and protection of Protected Health Information, shall survive the expiration or termination of this Agreement. The indemnity obligations specifically survive termination and remain enforceable thereafter. Covered Entity may set off any undisputed indemnified amounts against fees or other

sums otherwise due to Business Associate. Covered Entity also reserves the right, at its own option and expense, to participate in the defense of any claim, action, or proceeding through counsel of its choosing.

3. Mitigation and Cooperation.

(a) Business Associate's Duty to Mitigate. Business Associate shall promptly and at its sole cost mitigate damages resulting from violating this Agreement or the HIPAA Rules caused by the Business Associate or its agents or subcontractors. Mitigation includes technical remediation, operational containment, restoration of affected systems/data, and all actions necessary to reduce harm to individuals and Covered Entity.

(b) Timeliness and Standards. Mitigation shall begin without unreasonable delay and in accordance with Business Associate's written incident-response procedures and the HIPAA Breach Notification Rule (45 CFR Part 164, Subpart D – Notification in the Case of Breach of Unsecured Protected Health Information). Business Associate shall cooperate fully with Covered Entity and provide all information Covered Entity reasonably requests to complete the four-factor assessment under 45 CFR §164.402(2).

(c) Evidence Preservation. Business Associate shall preserve all potentially relevant logs, images, and records relating to any Security Incident or potential Breach for not less than six (6) years, and shall not destroy such evidence without Covered Entity's written consent.

4. Rights in Proprietary and Confidential Information

(a) Ownership. As between the parties, Covered Entity retains all rights, titles, and interests in and to the proprietary information, confidential information, and PROTECTED HEALTH INFORMATION provided to Business Associate. No rights are granted to Business Associate, its agent(s) or subcontractor(s), other than those expressly stated in this Agreement.

(b) Use Restrictions and No Analytics/AI Training. Business Associate shall not use Covered Entity's proprietary information, confidential information, or PROTECTED HEALTH INFORMATION for its own analytics, model training, product development, or other purposes as expressly authorized in writing by Covered Entity or permitted by law.

(c) Return/Destruction. Upon Covered Entity's request or upon termination/expiration, Business Associate shall return or securely destroy all Covered Entity information, including PROTECTED HEALTH INFORMATION, and certify completion within thirty (30) days, except as retention is Required by Law or a court order (in which case Business

Associate shall continue to protect such information in accordance with this Agreement).

(d) Injunctive Relief. Business Associate acknowledges that unauthorized use or disclosure of Covered Entity's proprietary information, confidential information, or Protected Health Information may cause irreparable harm for which monetary damages are inadequate. Covered Entity is therefore entitled to injunctive or equitable relief without posting bond in addition to all other remedies.

(e) Covered Entity's Limitation of Liability. Except for Covered Entity's gross negligence, willful misconduct, or breach of payment obligations, Covered Entity shall have no liability to Business Associate for consequential, incidental, special, punitive, or indirect damages, loss of profits, or loss of data, whether in contract, tort, or otherwise, even if advised of the possibility. Nothing in this clause limits Business Associate's obligations under this Agreement.

5. Cyber Liability Insurance.

Business Associate shall, at its sole cost, maintain Cyber and Privacy Liability Insurance with limits of not less than Five Million Dollars ($5,000,000) per claim and in the aggregate. Coverage shall, at a minimum, include:

- Privacy Liability – wrongful collection, use, retention, or disclosure of Protected Health Information or other personally identifiable information ("PII");
- Network Security Liability – unauthorized access, malware, denial-of-service, data corruption, or system interruption;
- Media and Content Liability – infringement, defamation, or digital-content risks;
- Regulatory Defense and Fines – defense costs and penalties to the extent insurable by law; and
- Incident Response and Breach Expenses – forensic investigation, notification, call-center, credit-monitoring, and data-restoration costs.

The policy shall:

- Name the City of Los Angeles ("City"), its departments, officers, and employees as additional insured where available at no additional cost;
- Be primary and non-contributory to any coverage carried by the City;
- Include no exclusion for unencrypted data or for acts of subcontractors;
- Remain in effect throughout the term of this Agreement and for not less than two (2) years following termination; and

- Require the insurer to provide at least 30 days' prior written notice to the City of cancellation, non-renewal, or material modification.

Upon request, Business Associate shall provide the City with a certificate of insurance and endorsements evidencing compliance and shall cooperate with the City's risk-management and legal teams in any claim investigation or recovery.

6. Survival.

The rights and obligations of the Parties under this Agreement, including those relating to the protection, return, or destruction of Protected Health Information, and any other provisions which by their nature should survive, shall survive the termination or expiration of this Agreement. Specifically, Business Associate's obligations with respect to the protection, use, disclosure, and retention of Covered Entity's Protected Health Information shall survive termination of this Agreement for as long as Business Associate retains any of such Protected Health Information and, in any event, for no less than six (6) years, consistent with 45 C.F.R. § 164.530(j)(2).

7. Retention.

This Agreement shall remain in effect for (i) the duration of Contract, if one exists between the Parties; or (ii) if no Contract exists, for the duration of the Services performed under this Agreement; and in either case, until all Protected Health Information created or received under this Agreement is returned to or destroyed at the direction of the Covered Entity, in accordance with 45 C.F.R. § 164.504(e)(2)(J).

8. Notices.

Any notices pertaining to this Agreement shall be given in writing and shall be deemed duly given when personally delivered to a Party or a Party's authorized representatives as listed below or sent by means of a reputable overnight carrier, or sent by means of certified mail, return receipt requested, postage prepaid. A notice sent by certified mail shall be deemed given on the date of receipt or refusal of receipt. All notices shall be addressed to the appropriate Party as follows:

If to Covered Entity (for Breach Notification):

Drew Steinberg, Public Safety Risk Manager (HIPAA Privacy Officer)
Los Angeles Fire Department
Risk Management Section
201 N. Figueroa St., 12th Floor

Los Angeles, CA 90012
(213) 202-9880

If to Covered Entity LAFD (For all other Matters)

Jaime E. Moore, Fire Chief
Los Angeles Fire Department
200 N. Main St., Room 1800
Los Angeles, California 90012
(213) 978-3800
(213) 978-3814 Fax

And:

Emilio Rodriguez, Fire Administrator
Los Angeles Fire Department
200 N. Main St., Room 1630
Los Angeles, California 90012
(213) 978-3731
(213) 978-3414 Fax

And:

If to Business Associate:

Mihir Desai, COO and CFO
3Di, Inc.
3 Pointe Drive, Suite 307
Brea, CA 92821
(714) 257-1100

H. MISCELLANEOUS

1. Amendment and Compliance.

The Parties shall amend this Agreement as necessary to comply with the HIPAA Rules, the HITECH Act, and any other applicable law or regulation. Any modification must be in writing and signed by duly authorized representatives of both Parties.

2. Duration and Survival.

This Agreement remains in effect for the duration of the underlying Contract or MOU and continues thereafter for so long as Business Associate retains any Protected Health Information on behalf of Covered Entity. All obligations relating to the use, protection, disclosure, retention, and

destruction of Protected Health Information survive termination until such Protected Health Information is securely destroyed in accordance with 45 C.F.R. §§ 164.504(e)(2)(J) and 164.530(j)(2).

3. Entire Agreement and Modification.

This Agreement, together with the underlying Contract, constitutes the entire agreement between the Parties regarding Protected Health Information. It supersedes all prior discussions or representations, oral or written. Any amendment or waiver must be in writing and executed by both Parties.

4. Governing Law.

Except to the extent pre-empted by federal law including HIPAA Rules, this Agreement and the rights and obligations of the Parties hereunder shall be governed by and construed in accordance with the laws of the State of California, consistent with the governing-law clause of the underlying Contract.

5. Assignment of Rights and Delegation of Duties.

This Agreement is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns. However, neither party may assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Notwithstanding any provisions to the contrary, however, Covered Entity retains the right to assign or delegate any of its rights or obligations hereunder to any City department or office in a manner consistent with the HIPAA Rules. Assignments made in violation of this provision are null and void.

6. Nature of the Agreement and Relationship of the Parties.

Nothing in this Agreement shall be construed to create (i) a partnership, joint venture, fiduciary, or employment relationship other joint business relationship between the Parties or any of their affiliates.

7. No Waiver.

Failure or delay on the part of either Party to exercise any right, power, privilege or remedy hereunder shall not constitute a waiver thereof. No provision of this Agreement may be waived by either Party except by a writing signed by an authorized representative of the Party making the waiver.

8. Equitable Relief.

Any disclosure of misappropriation of Protected Health Information by Business Associate in violation of this Agreement will cause Covered Entity irreparable harm, the amount of which may be difficult to ascertain. Business Associate therefore agrees that Covered Entity shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining Business Associate from any such further disclosure or breach, and for such other relief as Covered Entity shall deem appropriate. Such rights are in addition to any other remedies available to Covered Entity at law or in equity. Business Associate expressly waives the defense that a remedy in damages will be adequate, and further waives any requirement in an action for specific performance or injunction for the posting of a bond by Covered Entity.

9. Severability.

The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

10. No Third Party Beneficiaries.

Nothing in this Agreement shall be considered or construed as conferring any right or benefit on a person not party to this Agreement nor imposing any obligations on either Party hereto to persons not a party to this Agreement.

11. Headings.

The descriptive headings of the articles, sections, subsections of this Agreement are inserted for convenience only, do not constitute a part of this Agreement and shall not affect in any way the meaning or interpretation of this Agreement.

12. Inconsistencies.

Any inconsistency between this Agreement's provisions and the HIPAA Rules, including all amendments, as interpreted by HHS, a court, or another regulatory agency with authority over the Parties, shall be interpreted according to the interpretation of HHS, the court, or the regulatory agency. Any provisions of this Agreement that differs from those required by the HIPAA Rules, but is nonetheless permitted by the HIPAA Rules, shall be

adhered to as stated in this Agreement.

13. Regulatory References.

A citation in this Agreement to the Code of Federal Regulations shall mean the cited section as that section may be amended from time to time.

[SIGNATURE PAGE ON NEXT PAGE]

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized representatives.

THE CITY OF LOS ANGELES,
A Municipal Corporation

The signatory below has no personal, financial, beneficial, or familial interest in the contract.

By: _____
Jaime E. Moore
Los Angeles Fire Department
Fire Chief

Date: 8/18/2026

3Di, Inc., A California Corporation

By: _____
Rajiv Desai
President & C.E.O.

Date: July 24, 2026

By: _____
Mihir Desai (Jul 24, 2026 15:11:20 EDT)
Mihir Desai
C.O.O. & C.F.O.

Date: Jul 24, 2026

APPROVED AS TO FORM:
HYDEE FELDSTEIN SOTO,
City Attorney

By: _____
Benjamin Benhan
Deputy City Attorney

Date: 9/2/2026

*Approved signature methods for California corporations:

1) Two signatures: One of the Chairman of the Board of Directors, President, or Vice President, and one of the Secretary, Chief Financial Officer, or Assistant Treasurer.

2) One signature of a Corporate-designated individual together with a properly attested resolution of the Board of Directors authorizing the individual to sign.

ATTEST:
PATRICE Y. LATTIMORE, City Clerk

By: _____
Deputy City Clerk

Date: Sep 14, 2026

Agreement Number: C-205761

[Revised November 2025]

Annex A – Description of Services

(Attachment A to the Business Associate Agreement ("Agreement") between the City of Los Angeles by and through Los Angeles Fire Department ("Covered Entity" or "CE") and 3Di, Inc. ("Business Associate").

A.1. **General Information**

Field	Information to be completed by Business Associate
Business Associate Legal Name	**3Di, Inc.**
Primary Contact (Name / Title)	**Mihir Desai, COO and CFO**
Email / Phone	**ap@3disystems.com**
Business Address / Principal Office	**3 Pointe Drive, Suite 307 Brea, CA 92821**
Effective Date of Services	
City Department(s) Receiving Services	**Fire Department**
Related Contract / MOU Reference No.	

A.2. **Description of Services:** Provide a concise summary of the services Business Associate will perform on behalf of the City that involve access to, or the handling of, Protected Health Information (PHI).

City Department / Program	Description of Services Provided	Intended Purpose (e.g., Treatment, Payment, Operations)
LAFD - Los Angeles Fire Department	MRTS – Medical Records Request Tracking System	Provide software solution to LAFD staff to handle medical record request for protected medical information, including patient authorizations, legal subpoenas, law enforcement inquiries, regulatory agency requests, and 9-1-1 audio file releases.

(Note: Detailed data processing activities—including PHI elements, systems, and subcontractors—are documented in Annex B.)

A.3. **Key Deliverables:** List or describe deliverables to be produced under these services (e.g., billing reports, claims extracts, analytics summaries, audit logs, incident notifications).

Deliverable	Output Format	Frequency Recipient within City
MRTS Portal	Cloud hosted software solution	

A.4. **Authorized Personnel:** Identify key individuals responsible for program delivery and compliance.

Role / Function	Name/Title/Email/Phone/Contact Info.
Project Manager	**Pratik Desai** pratik.desai@3disystems.com +1 714.204.2221

A.5. **Subcontractor Overview:** Provide a list of agents or subcontracts handling PHI on behalf of Business Associate.

Subcontractor / Agent Name	Service Provided	Contact Information	Physical / Hosting Location	Access to PHI (Y/N)	Copy of Sub-Business Associate Agreement on File (Y/N)	CE Approval Date

A.6. **Change Management:** Business Associate shall notify CE **in writing** of any change to the services, scope, or subcontractor relationships described in this Annex A **within ten (10) business days** of such change.

Annex B – Data Processing Activities

(Attachment B to the Business Associate Agreement ("Agreement") between the City of Los Angeles by and through Los Angeles Fire Department ("Covered Entity" or "CE") and 3Di, Inc. ("Business Associate").

B.1. **Overview:** This Annex documents the specific processing activities performed by the Business Associate on behalf of the City of Los Angeles ("Covered Entity") that involve the creation, receipt, maintenance, or transmission of PHI, as required by 45 C.F.R. § 164.504(e).

B.2. Categories of PHI Processed

☑ Demographic data ☑ Medical / clinical ☑ Claims / billing ☐ Employee occupational health ☐ Limited data set ☐ Other (specify): _____

B.3. Data Processing Inventory

Activity/Function	Type of PHI Processed	Source of PHI (CE system or department)	Purpose of Processing	Retention Period
Medical Records Request Intake & Tracking	Demographic data (patient name, DOB, address, contact info, requestor identity)	Public requestors via MRRTS portal (patients, attorneys, law enforcement, agencies)	Health care operations – intake and tracking of EMS medical records disclosure requests per HIPAA/CMIA	Per LAFD records retention schedule.
PHI Collection, Review & Secure Release	Medical/clinical (EMS patient care reports, ePCR data, 9-1-1 audio recordings)	LAFD internal systems (ePCR, CAD/dispatch, billing, audio repositories)	Health care operations – gathering and securely releasing PHI to authorized requestors	Per LAFD retention schedule; auto-purge per configured rules.
Payment Processing for Records Request Fees	Limited demographic/billing data	Requestor-submitted via MRRTS portal	Fee collection (subpoena/processing fees) routed to EMS Accounting	Per LAFD retention schedule

B.4. Systems and Storage Environments

System / Application Name	Hosted By (Business Associate / Subcontractor / Cloud Provider)	Location (city/state or region)	Data Format (e.g., SQL, CSV)	Encryption at Rest (Y/N)	Encryption in Transit (Y/N)
3Di Engage – MRRTS	AWS (Cloud Provider) / 3Di, Inc.	us-west-1 (N. California) – Primary; us-west-2 (Oregon) – Cross-region	PostgreSQL (relational database)	Y	Y

		backup			

B.5. **Data Flow Summary:** Provide a general narrative or attach a diagram showing how PHI flows through your environment—from collection or receipt to storage, processing, disclosure, and destruction.

PHI enters via the MRRTS public portal when requestors submit medical records requests, uploading signed authorizations, subpoenas, or identity documents. Data is transmitted over TLS 1.2/1.3 to AWS us-west-1 encrypted SQL databases (AES-256/FIPS 140-2). LAFD staff collect requested PHI (EMS patient care records, ePCR, 9-1-1 audio) from LAFD internal systems, review for completeness, and release securely via encrypted portal. All PHI access is logged in immutable audit trails. PHI is retained per LAFD-configured schedules, automatically archived and purged. Backups replicate every 12 hours to us-west-2 (Oregon), retained 7 days.

B.6. **Safeguards Summary:** Summarize or reference your latest risk assessment.

- **Administrative Controls:** Role-based access control (RBAC) policies; mandatory security awareness training on hire and annually; periodic user access reviews; written incident response and vulnerability management policies; SOC 2 Type II certified (Security, Confidentiality, Availability, Processing Integrity, Privacy)
- **Physical Controls:** All PHI hosted exclusively in AWS data centers with AWS-managed physical access controls; no on-premises PHI storage; physical access limited to authorized AWS personnel per SOC 2 controls
- **Technical Controls:** FIPS 140-2 AES-256 encryption at rest (AWS KMS); TLS 1.2 encryption in transit; OAuth2 identity management with MFA; RBAC; dedicated VPC with public/private subnet isolation; OWASP Top 10-compliant Layer 7 WAF; AWS CloudTrail and CloudWatch audit logging; AWS GuardDuty intrusion detection; centralized credential management via AWS Parameter Store

B.7. **Retention and Disposal**

Data Type	**Retention Period**	**Disposal Method (e.g., shredding, cryptographic wipe)**	**Responsible Party**
EMS medical records / PHI (patient care reports, demographics, case documents)	Per LAFD retention schedule and HIPAA requirements; auto-archived/purged per MRRTS retention rules	Automated purge per retention rules; cryptographic wipe via AWS KMS key deletion on contract termination	3Di, Inc.
Backup snapshots (containing PHI)	7 days	Automated AWS snapshot expiration	3Di, Inc.

B.8. **Change and Notification Obligations:** Business Associate must promptly notify Covered Entity of:

- Any addition / change of subcontractor or system involving PHI;
- Any change in storage location or data flow; or
- Any security incident as defined in 45 C.F.R. § 164.304.

B.9. **Certification:** Business Associate certifies that:

- The information in this Annex B is complete and accurate;
- All systems and subcontractors listed comply with the HIPAA Security Rule (45 C.F.R. §§ 164.308–164.312); and
- Business Associate will provide an updated Annex B within ten (10) business days of any material change.

Annex C – Security Incident and Breach Information

(Attachment C to the Business Associate Agreement (Agreement) between the City of Los Angeles by and through Los Angeles Fire Department ("Covered Entity" or "CE") and 3Di, Inc. ("Business Associate").

C.1. **Purpose:** This Annex documents how Business Associate will detect, report, and coordinate with the City of Los Angeles ("Covered Entity") in the event of a Security Incident or Breach involving Protected Health Information (PHI) or electronic PHI (ePHI). It also serves as the template for incident notification and post-incident documentation.

C.2. Key Regulatory References

- 45 C.F.R. § 164.304 – Definition of "Security Incident."
- 45 C.F.R. § 164.308(a)(6) – Security Incident procedures (response & reporting).
- 45 C.F.R. § 164.402–410 – Breach Notification Rule requirements.

C.3. Designated Points of Contact

Role	Organization	Name / Title	Email / Phone	24/7 Contact (Y/N)
Business Associate Incident Response Lead	3Di, Inc.	Amit Brahmbhatt, VP Product Development	security@3disystems.com +1 (253) 334-9008	Y
Business Associate Security Officer	3Di, Inc.	Piyush Gandhi, CISO	security@3disystems.com +1 (714) 494-7509	Y
Business Associate Privacy Officer	3Di, Inc.	Piyush Gandhi, CISO	security@3disystems.com +1 (714) 494-7509	Y
CE HIPAA Privacy Officer	City of Los Angeles			
CE CISO / ITA Cyber Ops	City of Los Angeles			

C.4. Reporting Obligations

Event Type	Initial Notice Due to CE	Content Required	Follow-Up Report Due
Suspected Security Incident	Within 72 hours of discovery	Description, date/time, systems/data involved, containment actions, contact person	Within 5 business days with preliminary findings
Confirmed Security Incident	Immediate (≤ 72 hours)	Expanded details, root cause in progress	Within 5 business days with root-cause analysis + corrective plan
Breach of Unsecured PHI (45 C.F.R. § 164.402)	Immediate notification (≤ 72 hours)	All data elements required under § 164.410(c): nature of PHI, individuals affected, timing, mitigation, actions taken	Comprehensive written report within 10 business days
Suspected Security Incident	Within 72 hours of discovery	Description, date/time, systems/data involved, containment actions, contact person	Within 5 business days with preliminary findings

C.5. **Incident Information Form:** *(to be completed by Business Associate and submitted with initial notice)*

Field	Information to be Provided by Business Associate
Date / Time Discovered	
Date / Time Occurred (if known)	
Detection Method (e.g., SIEM alert, user report)	
Type of Incident (e.g., ransomware, phishing, unauthorized access)	
Systems / Applications Affected	
Approx. Records Affected (# individuals)	
Containment Actions Taken	
Current Status (ongoing, contained, eradicated)	
External Parties Notified (LE, regulators, insurers)	
Evidence Preservation Steps	
Incident Lead Name / Contact	

(Attach additional pages or supporting documentation as needed.)

C.6. **Coordination and Investigation**

- Joint Response: Business Associate shall cooperate fully with CE, its designated representatives, and law enforcement in investigating and remediating any incident.
- Evidence Preservation: Business Associate must preserve logs, emails, forensic images, and related records for at least six (6) years from discovery of the incident.
- No Public Statements: Business Associate shall not make any public disclosure about the incident without CE's written consent.

C.7. **Breach Determination and Notification:** If Business Associate determines—or CE reasonably believes—that an incident constitutes a Breach of Unsecured PHI, Business Associate shall:

1. Immediately notify CE as above;
2. Provide CE with a draft notification package containing all information required by 45 C.F.R. § 164.410(c); and
3. Refrain from issuing any notifications to individuals or regulators without CE's written direction.

C.8. **Corrective Action and Lessons Learned:** Within ten (10) business days after incident closure, Business Associate shall submit to CE a written Root Cause Analysis and Corrective Action Plan, including any security control changes, training, or policy updates implemented as a result of the incident.

C.9. **Ongoing Reporting and Metrics:** Business Associate shall provide to CE, upon request:

- A summary of all Security Incidents for the preceding twelve (12) months (including near misses);
- Evidence of incident response testing or tabletop exercises performed within the past year; and
- Contact updates for incident response personnel.

C.10. **Certification:** The Business Associate certifies that:

- It has established, documented, and tested incident response procedures consistent with 45 C.F.R. § 164.308(a)(6);
- All information reported herein is accurate to the best of its knowledge; and
- It will promptly update this Annex should its incident response contacts or procedures change.

Annex D – Artificial Intelligence ("AI") System and Automated Processing

(Attachment D to the Business Associate Agreement ("Agreement") between the City of Los Angeles by and through Los Angeles Fire Department ("Covered Entity") and 3Di, Inc. ("Business Associate").

D.1. **Purpose:** This Annex documents and governs AI System, Machine Learning ("ML"), or other automated data-processing activities performed by Business Associate that exclusively involve, rely upon, or are derived from Protected Health Information entrusted by the City of Los Angeles. (To the extent AI System and Automated Processing does not involving Protected Health Information, Business Associate's general AI system activities fall outside the scope of this Agreement.)

D.2. **Key Regulatory References**

- 45 C.F.R. §§164.308-312 (security safeguards).
- 45 C.F.R. §164.514(b) (de-identification methodology), and
- Applicable state or municipal data-governance laws (e.g., California Privacy Rights Act, California AI procurement guidance).

D.3. **Definitions**

Applicable definitions describing AI System, Automated Processing, or Automated Decision Systems (ADS) are outlined in the Definition Section of the Agreement.

D.4. Disclosure of AI or Automated Processing *(to be completed by Business Associate)*

System/Tool name	Vendor/Deployer	Purpose/Use Case	PHI Input or Derived Data Used Categories	Output/Decisions Produced	Human Intervention
Not Applicable	N/A	Business Associate does not use AI, ML, or automated decision-making involving PHI	N/A	N/A	N/A

D.4. **Authorized and Prohibited Uses**

Authorized uses with Covered Entity's written approval:

- Performing Covered Entity-approved treatment, payment, or health-care operations under 45 C.F.R. §164.506(c).
- Performing limited quality or operational analytics solely for Covered Entity's benefit.

Prohibited uses:

- Training, fine-tuning, or validating general-purpose, commercial, or generative AI models.

- Combining Covered Entity with other clients' data or external sources.
- Creating synthetic or de-identified data for independent use without Covered Entity's written authorization.
- Any automated decision that affects individuals without human review or Covered Entity's oversight.

D.5. **Transparency and Documentation**

- Provide plain language description of each AI/ADS system's purpose, inputs and logic request.:

- Provide documentation of de-identification methodology (Expert Determination or Safe Harbor) per 45 C.F.R. §164.514(b).:

- Provide proof that you maintain internal model-risk and bias-assessment documentation, updated annually or after any material change where Covered Entity's data, including PHI, is in scope.:

D.6. **Safeguard and Data Integrity**

Business Associate shall:

- Apply HIPAA Security Rule safeguards (45 C.F.R. §164.308-312) to all systems using or storing PHI.
- Encrypt PHI at rest and in transit (FIPS 140-2 or successor).
- Implement logging, access control, and audit trails for training, inference, and model-output use.
- Ensure segregation of Covered Entity PHI datasets from test or sandbox, other clients, or public data environments.

- Monitor for model drifts, data leakages, inversions, or biases and report material findings to Covered Entity.

D.7. **Subcontractors and AI Vendors**: List any third parties or vendors supporting AI or automated processing of PHI.

Subcontractor/Vendor Name	Role/Function	System or Model Used	Location/Hosting Region

All such parties must be bound by written agreements imposing HIPAA-equivalent obligations and are subject to CE's prior written approval.

D.8. **Incident Reporting**: Any algorithmic malfunction, bias event, unauthorized access (to the data, model, test/production env., etc.), or other incident affecting PHI integrity or system behavior shall be treated as a Security Incident under Annex C and reported within the same timelines.

D.9. **Oversight and Audit**

Covered Entity may:

- Audit Business Associate's AI systems and related controls.
- Require suspension of any high-risk automated processing.
- Request copies of model documentation and validation results.

D.10. **Certification**

The Business Associate certifies that:

- All AI and automated systems handling Covered Entity data comply with HIPAA, this Agreement, and applicable laws, standards and policies.
- Covered Entity will be notified within ten (10) business days of any new or materially changed automated-processing activity.
- Human oversight (including Human-in-the-loop and Human-on-the-loop) and decision transparency, fairness, and accountability are maintained at all times.