International Workshop on Interoperability and Rescue

PFIF and EDXL: Interoperability of Person Registering and Tracing Systems

Dr. Antonis Kostaridis
CTO
Satways Ltd.

www.satways.net

Outline

- Disaster aftermath problems
- How technology can help?
- Missing Person Registries
- The need for interoperability and standardization
- Interoperable Missing Person Data Exchange Registries
- PFIF Overview
- EDXL-TEP/TEC Emerging Standards
- IDIRA support for missing person tracing
- Conclusions

Disaster Aftermath Problems

Disaster by definition is that which exceeds the capacity of local emergency services

Problems:

- The trauma caused by waiting to be found or find next of kin
- Coordinating all response groups by helping them to operate effectively as a whole
- Managing the multitude of requests from the affected region and matching them effectively to the pledges of assistance
- Tracking the location of all temporary shelters, camps, etc.

How Technology can Help?

- **Establish communication channels**
  - Even ad-hoc communications when existing infrastructure has been damaged
- **Scalable electronic management of information**
  - No stacks of form and files to manage
- **Efficient distribution of information**
  - Accessibility of information on demand
- **Automatic collation and calculation**
  - Minimize delays for assessments and calculations
- **Real-time situational awareness**
  - Reports are updated live as data is entered

Missing Person Registries

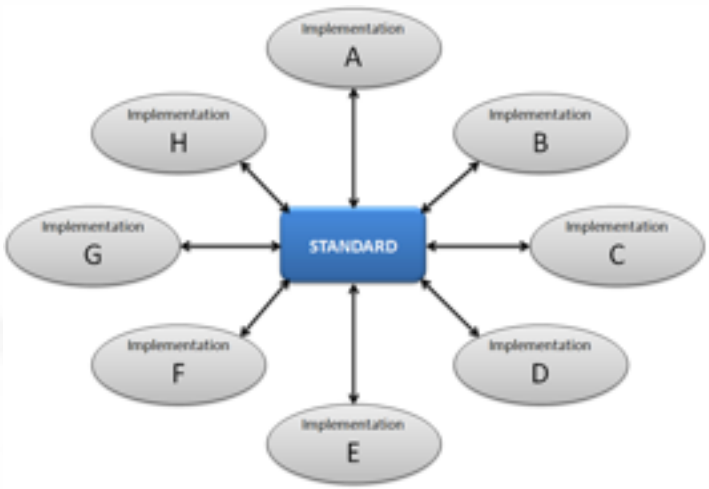
- Helps track and find missing, deceased, injured and displaced people and families
- Be able to record all structured meta data on a victim (pictures and biometric data)
- Indexing and Searching of all data

Significance of Tracking Victims

- Whole disaster management process is based on accurate/available people information
- Request aid management significantly depends on the people information
  - Donors can provide necessary items
  - Requests duplication can be eliminated
- Increase the efficiency of Volunteers
  - Proper volunteer allocation
  - Accelerate the relief process

The need of Interoperability and Standards

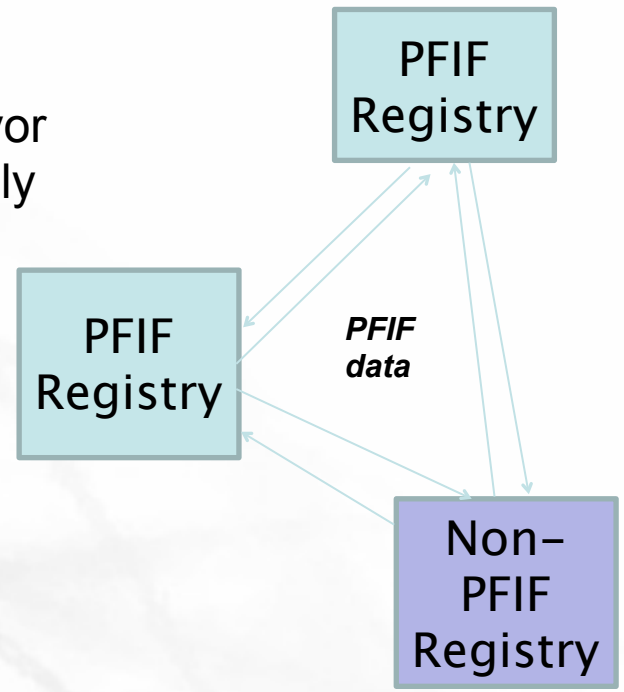
- Multiple repositories of information arise during disasters due to multiple reasons
  - Unavailability of appropriate systems
  - Trust and relationship with organization
  - Capacity of organization to respond
- Bring out effective information exchange during crisis to prevent siloed repositories that is of less value to response
- Better efficiency in finding missing people especially in the critical first 72 hours.
- Less time wasted avoiding data re-entry
- Better collaboration between relief agencies



PFIF Introduction

PFIF: Person Finder Interchange Format

- Designed to enable information sharing among governments, relief organizations, and other survivor registries to help people find and contact their family and friends after a disaster.
- XML data model
- Current version: 1.3 (2011/03/07)
- XML records can be embedded in Atom feeds or RSS feeds.
- Specification for data synchronization between different repositories



PFIF Origins

September 11 attacks (2001)

- 25 different online forums and survivor registries
- safe.millenium.berkley.edu was the largest survivor registry (by graduate students Ka-Ping Yee and Miriam Walker).
- collection of information from different databases required manual effort and custom programming

After Hurricane Katrina (2005)

- Again 25 many online forums and survivor registries
- Large volunteer effort called the **Katrina PeopleFinder** project (salesforce.com database)
- Together with volunteers and the CiviCRM team, Ka-Ping Yee developed the first draft of the PFIF spec (1.0, 1.1)

PFIF Design Principles (1)

Convergence

- of people who seek the same person
- of information about a person obtained from various sources
- of duplicated data
- of missing people with their loved ones

Data should be traceable: Since data comes from sources of unknown reliability and accountability, information on the origins of data should be maintained, to help users ascertain its trustworthiness.

Track of origin:

- Each record belongs to an original repository, which is the (PFIF or non-PFIF) repository where the record was first entered.
- The record may be copied to other places, but the original repository remains the authority on the record.
- Only the original repository should ever change the contents of a record.

PFIF Design Principles (2)

Flexibility: Each aggregator of data has its own perspective on the world and is responsible for choosing which data sources to trust. It is not possible to dictate truths about all data from a single central authority.

Association: Because multiple records might refer to the same person, PFIF allows such records to be associated with each other. But, by the preceding principle, each aggregator makes its own decisions about which records to associate; there is no central authority.

Merging: It should be possible to resolve multiple copies of the same record that have been imported via different data paths.

Time reference: All dates and times must be in UTC, never in a local time zone, because data records will be transmitted among many different time zones.

PFIF: Haiti Case Study

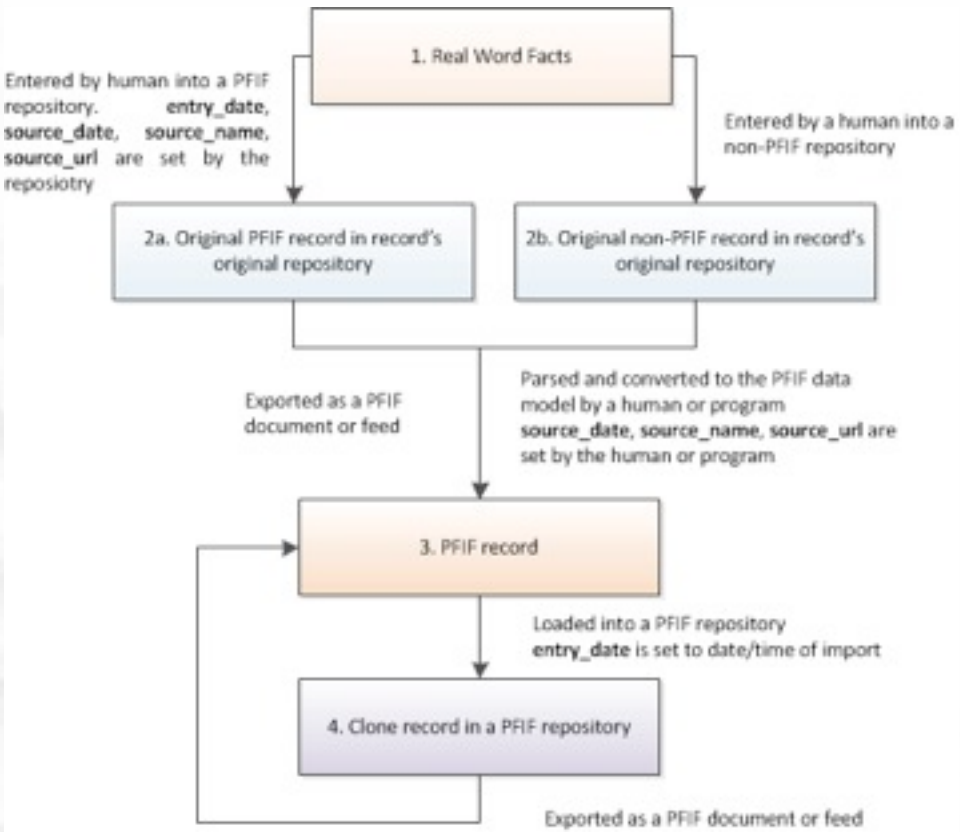
- **HELP: Haiti Earthquake People Locator**
- **Google Person Finder**

PFIF

PFIF Data Lifecycle

Each PFIF repository may contain **original** records and **clone** records.

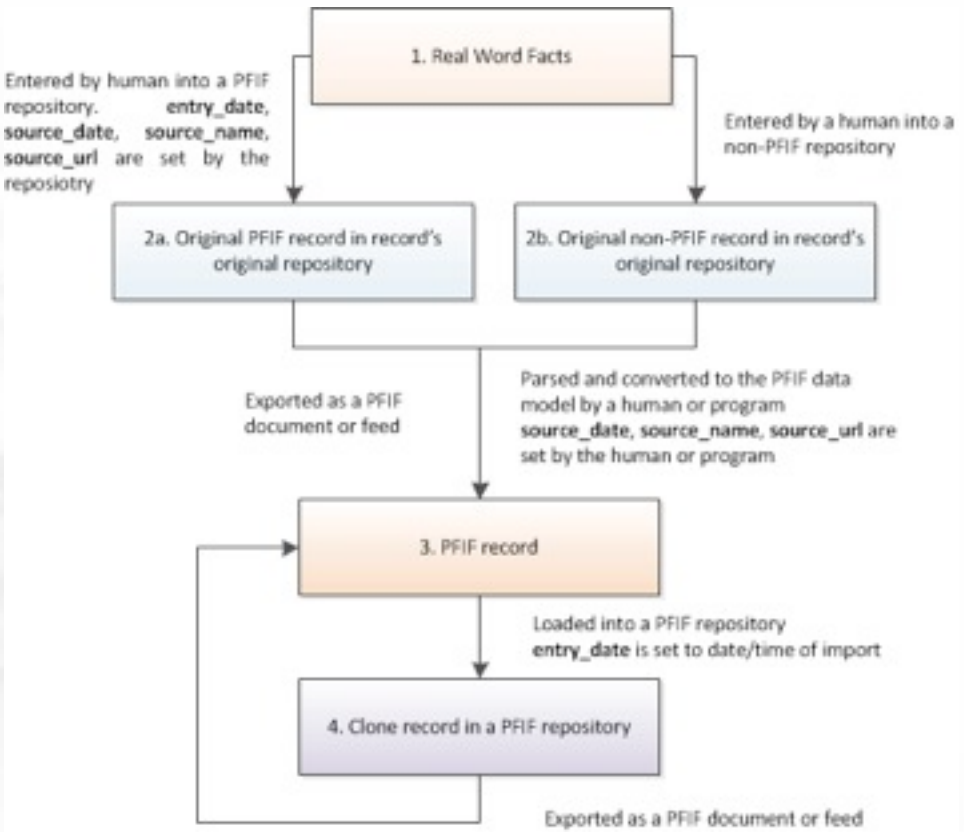
- an original record is a record residing in its original repository
- a clone record is a copy of a record that originated in another repository.



PFIF Data Update Mechanism

- The original repository for a record (2a or 2b) can update any of the fields on a record after it is created, except the **person_record_id** field.

- Whenever a PFIF repository creates or updates an original record, it must set both the **source_date** and **entry_date** to the current time. When a repository imports a PFIF record that has the same record identifier as an existing record, it should keep the version with the latest **source_date**.



PFIF: Data Expiry Mechanism (1)

If present, the expiry_date field indicates when a record should be deleted to preserve the privacy of the personal information it contains. Conforming PFIF implementations must meet the following requirements:

- Within one day after expiry_date, a PFIF repository must make the contents of the PERSON record and any associated NOTE records inaccessible to all external clients, including users and machine API clients.

- Thereafter, if the repository exports its data through an API, it should continue to export a placeholder record in the place of the expired PERSON record. This placeholder should keep the same person_record_id and expiry_date values, and have both source_date and entry_date set to the time that the placeholder was created. All other fields should be empty or omitted.

PFIF: Data Expiry Mechanism (2)

- Within 60 days after expiry_date, a PFIF repository must permanently and unrecoverably delete all its copies (including backups) of the contents of the PERSON record and any associated NOTE records, except for the person_record_id, source_date, entry_date, and expiry_date fields needed to produce the placeholder.

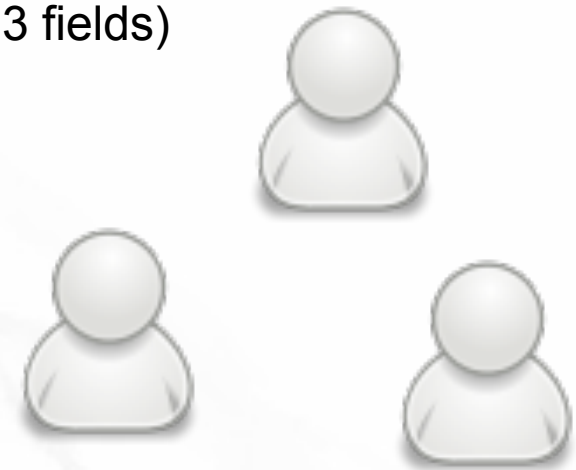
- To satisfy a user request to delete an existing original record, a PFIF repository should set the record's expiry_date to the current time. This causes the deletion to propagate to other conforming PFIF repositories.

PFIF Data Model (1)

- Person Record (23 fields in total)
  - Metadata about the record itself (9 fields)
    - person_record_id
    - entry_date
    - expiry_date
    - author_name
    - author_email
    - author_phone
    - source_name
    - source_date
    - source_url

PFIF Data Model (2)

- Person Record
  - Identifying information about a missing person (13 fields)
    - full_name
    - first_name
    - last_name
    - sex
    - date_of_birth
    - age
    - home_street
    - photo_url
    - e.t.c.

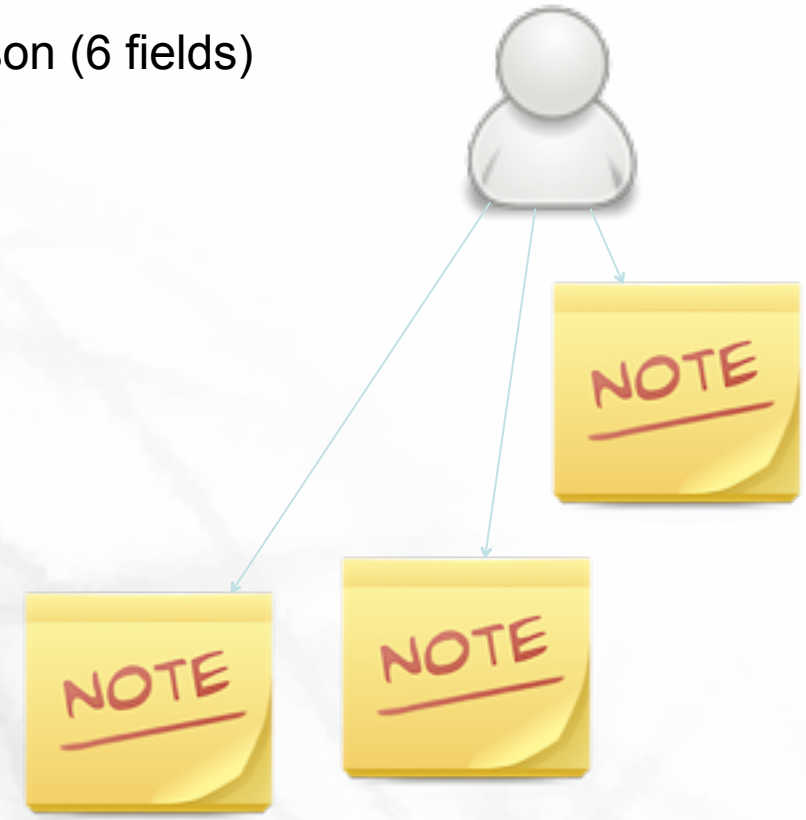


PFIF Data Model (3)

- Notes Records (14 fields in total)
  - Metadata about the record itself (8 fields)
    - Nore_record_id
    - Person_record_id
    - Lnked_person_id
    - Entry_date
    - Author_name
    - Author_email
    - Author_phone
    - Source_date

PFIF Data Model (4)

- Notes Records
  - Status information about the missing person (6 fields)
    - Found
    - Status
    - Email_of_found_person
    - Phone_of_found_person
    - Last_known_location
    - text



PFIF Example UI

Emergency Data Exchange Language (EDXL)

EDXL

- Suite of messaging standards with technical rules governing how emergency-related information is packaged for exchange
- Cannot change systems / database to “speak the same language”
- XML-based, not a new XML “language” and not “data standards”
- Open Process, Cross-profession, All-hazards

EDXL Implementation

- Systems receive and send information using these standards
- Information is displayed in the native system user-friendly format
- Utilize Open Application Programming Interfaces

EDXL Standards

OASIS: Organization for the Advancement of Structured Information Standards

Common Alerting Protocol (CAP) - An XML message for exchange of emergency alerts, notifications, and public warnings

Distribution Element (DE) – Easy wrap and route of any EDXL or other emergency information (XML and non-XML). "Address" the package in flexible ways to support intelligent routing by roles, geographic area, or keywords

Resource Messaging (RM) - OASIS standard in November 2008. A suite of 16 standard XML formats for exchange of emergency resource information (equipment, supplies, people, and teams).

Hospital AVailability Exchange (HAVE) - OASIS standard in November 2008. An XML message for exchange of hospital status, services and resources. Assists hospital coordination and routing of patients to facilities for care during emergencies

Situation Reporting (SitRep) - Submitted from practitioner process to OASIS in April 2009 and **in-process**. An XML message for exchange of situation / incident / event and response information.

EDXL – TEP/TEC

Requirements definition for Tracking of Emergency Patients and Tracking of Emergency Clients is occurring in two phases.

Phase I - Tracking of Emergency Patients (TEP): An XML standard for exchange of emergency patient and EMS tracking information to increase:

- the effectiveness of emergency medical management
- patient tracking and care
- family notification.

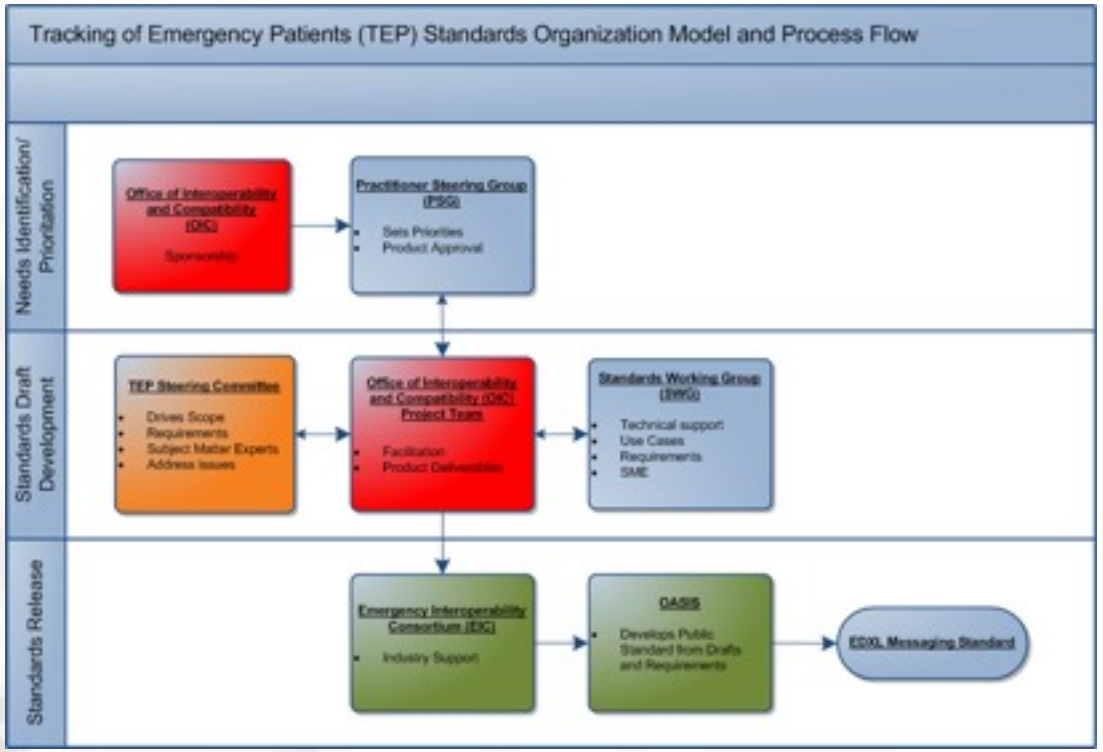
Phase II - Tracking of Emergency Clients (TEC): Expands Phase I scope to support clients across the general population. TEC is aimed at more effective:

- evacuation and services management
- client tracking
- regulation
- re-unification
- use of assets for all Emergency clients.

EDXL – TEP/TEC

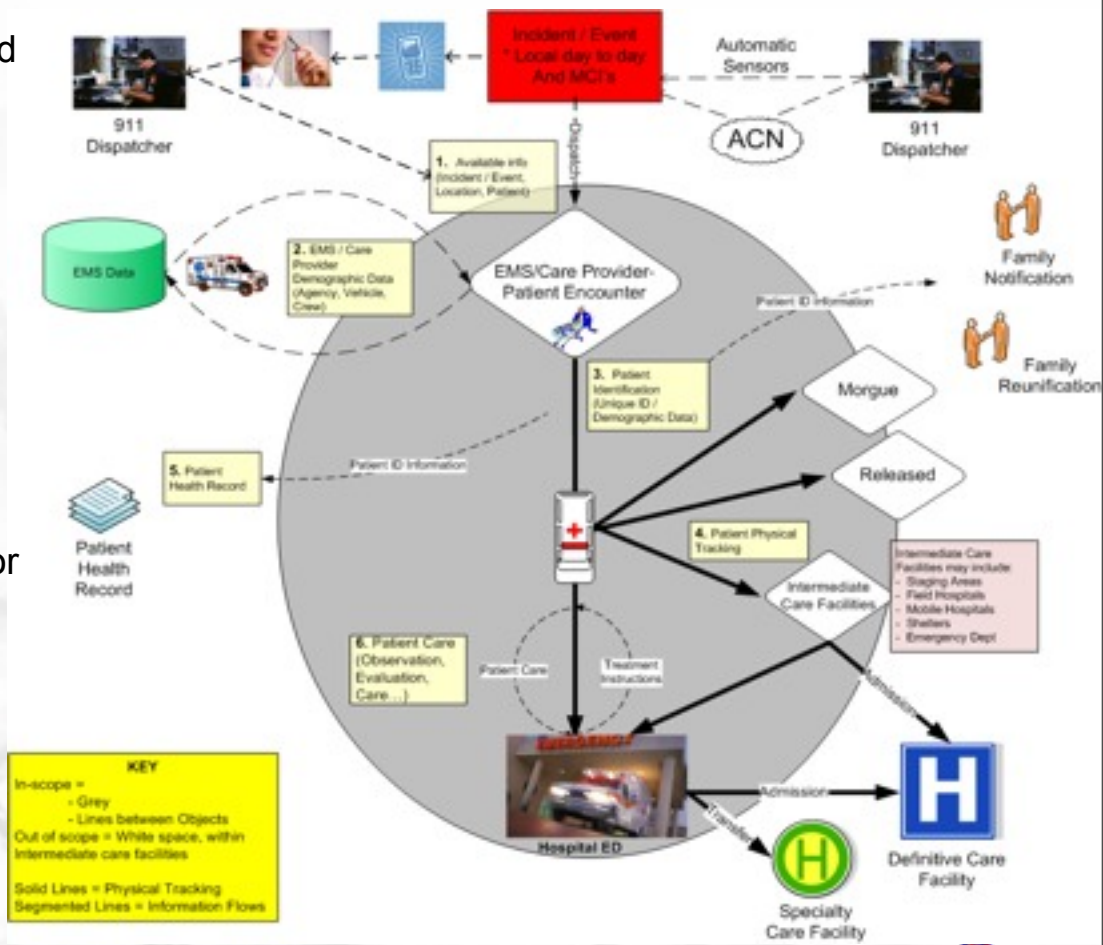
Client: Generic term for any person displaced, evacuated, sheltering in place, expired, and/or requiring medical attention – i.e. Clients or customers of Emergency Services

Patient: A type of client requiring medical attention, being medically evaluated; or a fatality .



EDXL-TEP Scope

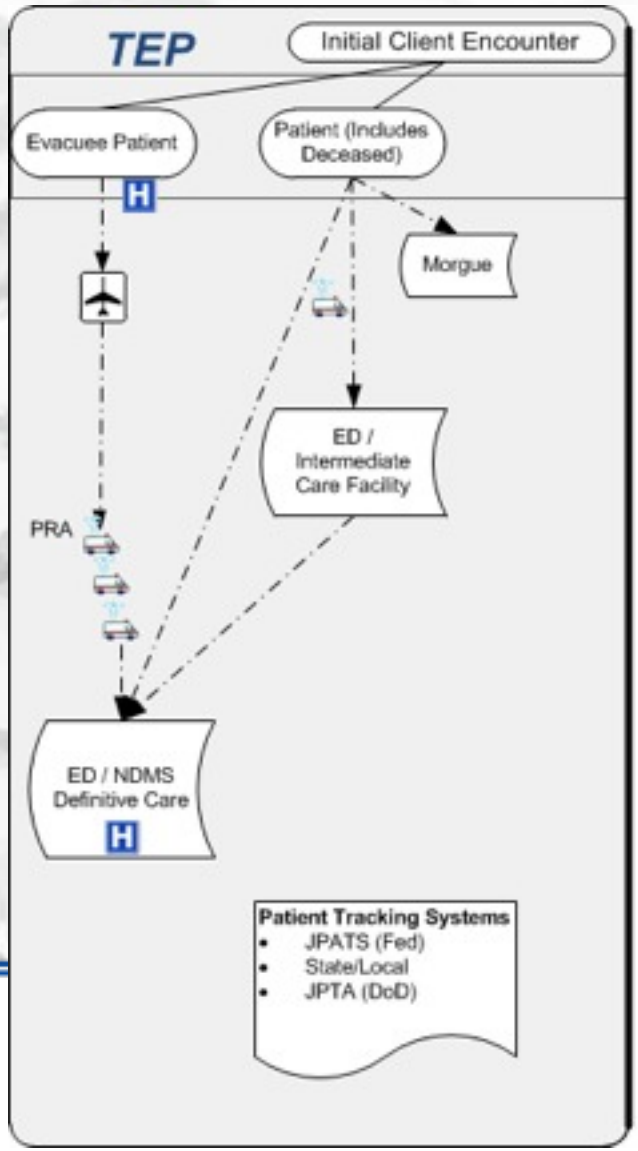
- EDXL-TEP is an XML messaging standard for exchange of emergency patient and tracking information across the EMS emergency medical care continuum.
- TEP provides real-time information to responders, management and care facilities in the chain of emergency care and transport.
- Patient tracking information is exchanged from patient encounter (possibly re-using dispatch information) through admission or release.
- TEP also supports hospital evacuations and day to day patient transfers.

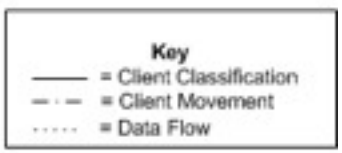


EDXL-TEC Scope

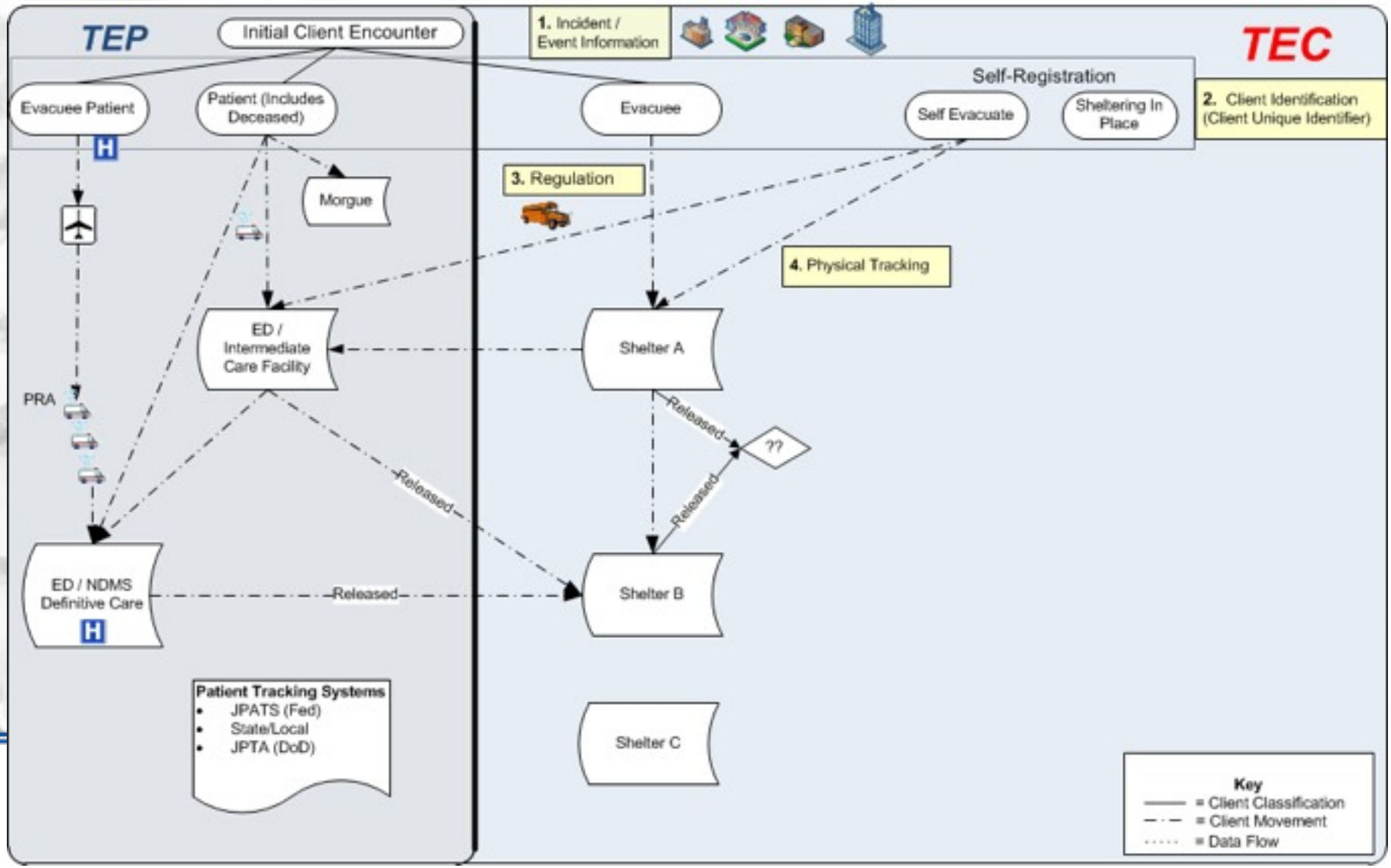
- Expands Phase I scope to support clients across the general population for more effective evacuation and services management.
- Provides real-time information to responders, decision-makers, and facilities in the chain of care and transport.
- TEC primary objectives include the following:
  - Non-medical evacuee movement & tracking (also self-evacuees and shelter-in-place)
  - Regulation
  - "Richer" data sources
    - Person finding
    - Family notification & re-unification
    - Sharing of "self-registration" data

EDXL-TEC Generic Process

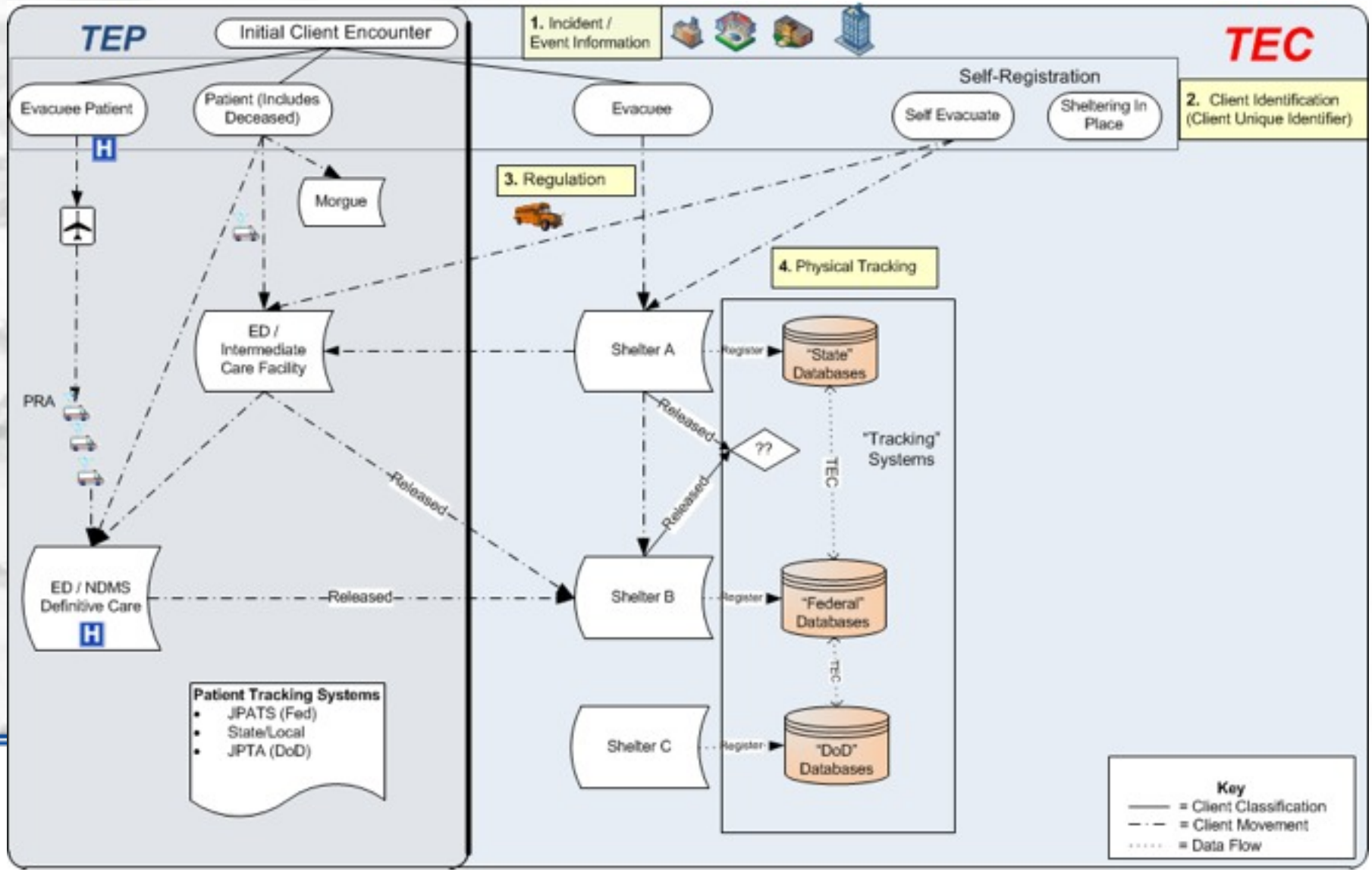




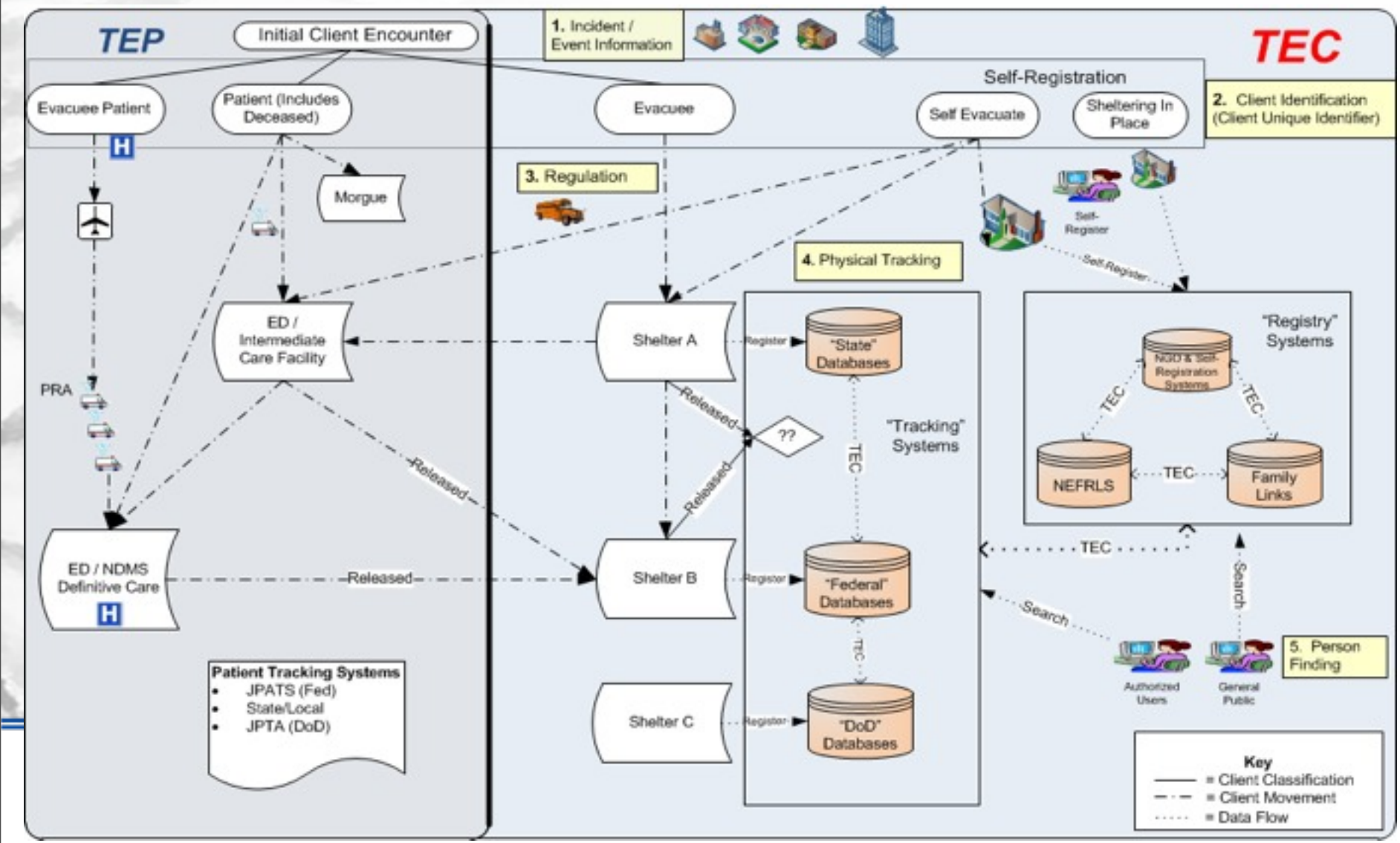
EDXL-TEC/TEP Generic Process



EDXL-TEC Generic Process



EDXL-TEC Generic Process

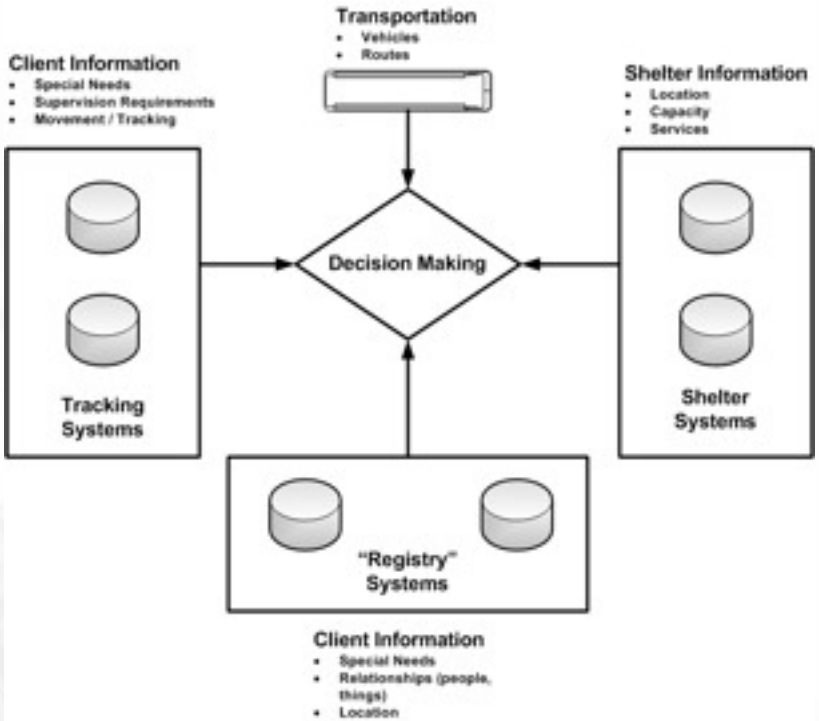


EDXL-TEC Possible Messages (1)

1. Client Movement/Tracking

Usage:

1. Evacuee encounters, transport / departure, arrival, etc.
2. Sent to other tracking and/or registry systems. Info used to match needs with transportation and shelter availability. Similar to TEP equivalent for patient tracking from one location to the next.



2. Client "Registry" Information

New or updated info sent from one registry system to another, to enrich the evacuee information across registries and increase the usefulness of people finding applications, family reunification and family notification **(adoption of PFIF in whole or in part as component of message).**

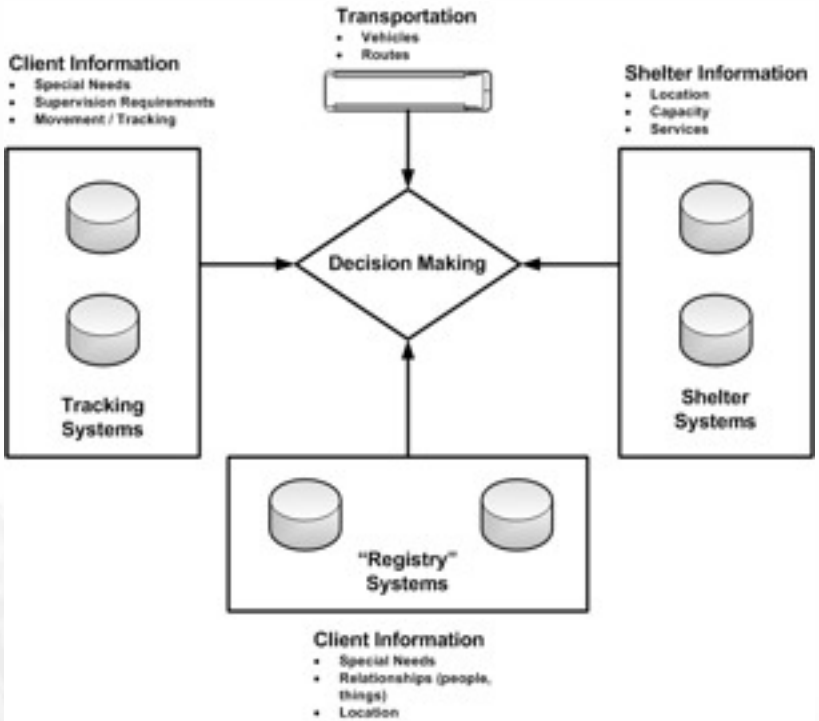
EDXL-TEC Possible Messages (2)

3. Shelter Availability

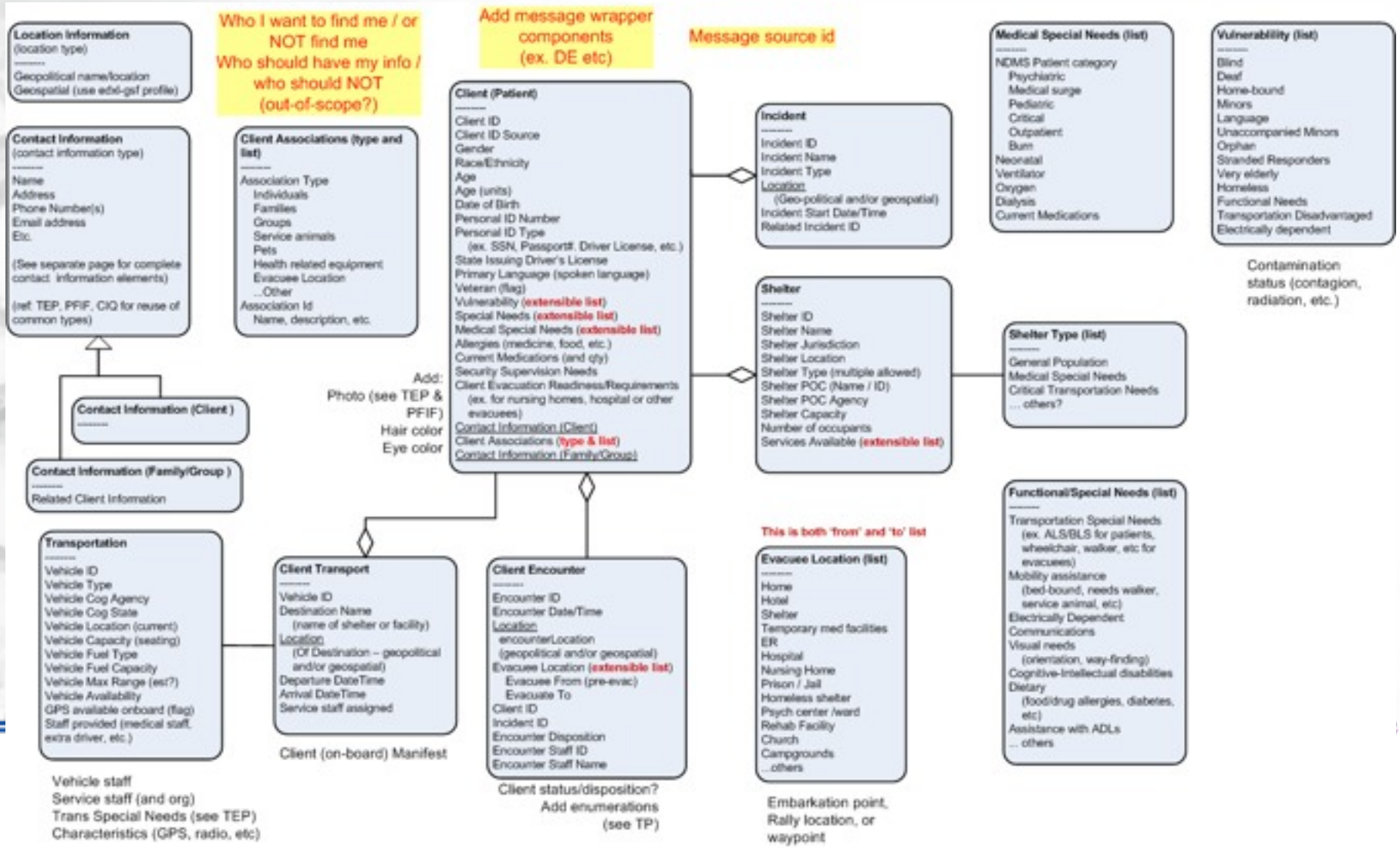
Provide evacuation management and info about shelter options in order to better match evacuee needs with possible shelter destinations. Also provide info about current population of shelter versus their available capacity.

4. Transport Availability & Regulation

Same as Shelter Availability, except for transportation options. Availability of transport (Air-fixed wing, air-rotor, ambulance, bus, water - ship etc. What info and to what level of detail?



EDXL-TEC: Draft "Data View"



IDIRA and Missing Person Tracing

- Adoption of PFIF 1.3 / 1.4
- Follow EDXL-TEP/TEC evolution during project development
- Enable the registration and search of missing person data from mobile devices (tablets, phones)
- Enable the interoperability of XENIOS (Red Cross), C&C systems and PFIF repositories (like Google Person Finder).

Conclusions

- PFIF and EDXL-TEC/TEP will probably will co-exist and cover different needs
- There a lot of emerging standards in the crisis response domain
- Even when mature, the implementation of the standards can be immature
- Data exchange standards are not used frequently and only during a crisis event
- Frequent workshops activity that will prove readiness between systems for data exchange during a crisis are needed

Thank you