# Initial Guidance for End Users on Remote Temperature Monitoring Systems – Part One

Considerations for implementation of systems

## Questions to ask

Is the hardware fit for purpose?

- How do the sensors measure temperature? E.g. is it by contact probes, probe pockets, immersion, etc.?
- Is this method of measurement suitable for my pipe material and size?
- How are the sensors installed? Is there any risk of them becoming separated from the pipe?
- Will the sensors and other associated equipment communicate through my building? You may need to tell the supplier what your building is constructed from and how thick walls and floors are.
- How often does the equipment require replacement batteries or verification?
- How easy is it to maintain?
- How can you tell if a sensor is malfunctioning?
- How does frequency of measurement affect the battery life?
- How long will sensors be supported by the supplier, and what happens when they are superseded?

How is the data delivered?

- Is there a time delay between a reading and delivery to the interface?
- Is data robustly backed up? Where is data stored? UK? Security considerations.
- What data is provided? All data or high/low/average figures?
- How frequently are measurements taken?
- Does data transfer require a cabled network connection to the sensors?
- How user friendly is the interface? This is subjective but important.
- Can the interface manipulate data to generate reports? Can it export data in usable formats such as CSV files?
- Can the interface generate alerts/non-conformances and how are these managed? Do these meet the requirements of the existing Legionella risk management guidance? Are they user configurable?
- How reliable is data transfer?
- Is data transfer reliant on a customer's own local network and/or internet connection?
- Can the system be integrated with existing water hygiene management software or building management systems?
- At the end of the contract who owns the data? And can it still be accessed for 5 years from the time of data collection, as required by COSHH?

How is the system designed and installed?

- Where will sensors be located and have these decisions been made by those with an understanding of the building water systems installed, the people using these systems, the Legionella risk assessment and the guidance in place?
- Are there enough sensors to give a useful thermal profile that informs on the Legionella risk?
- Will the placement of sensors be prone to damage, vandalism, unintentional switch off, etc.?
- Are the sensors invasive/intrusive?
- Do the sensors require access to an external power source to operate?
- Who will install the system, are they competent to do so, can you provide evidence for this?
- How will the system be commissioned? How will the system be calibrated?

- Is the supplier able to provide ongoing technical and practical support?
- Who is responsible for training the end user? Both initially and after system upgrades/updates?

Security considerations (these may be internal questions or a conversation with the supplier)

- Will this system's communication interfere with other systems on the premises?
- Is this type of equipment permitted at my site under the site security conditions?
- How secure is the data transfer, e.g. end-to-end encryption, 2 factor authentication for end user?

Communication

- What is the best communication method for my application? (WiFi, BLE, NBIOT, low frequency, cellular etc.)
- What are the ongoing communication costs?
- What is the network coverage in my area?

Environmental

- How much of the product is recyclable?
- What is the carbon footprint of the supply chain?
- How does the carbon footprint compare with existing manual monitoring?

Financial

- How much does the system cost over its lifespan?
- Lease or purchase? Operational expenditure versus capital expenditure.
- What are the likely ongoing costs of support?
- What does the warranty cover?
- What is the ongoing cost of access to the software?

# Is the hardware fit for purpose?

## How do the sensors measure temperature? E.g. is it by contact probes, probe pockets, immersion, etc.?

Our remote monitoring sensors, Clip'R and Strap'R measure the temperature by using contact probes measuring the temperature of a metal pipe and thus the temperature of the water inside with a small deviation.

## Is this method of measurement suitable for my pipe material and size?

You can use our sensors on any metal piping material. Plastic and PVC do not work for our sensors. When this is the case, it is recommended to place a metal fitting in between to ensure correct, accurate measurement.

## How are the sensors installed? Is there any risk of them becoming separated from the pipe?

The sensors are installed by clipping the sensors to the pipe. The only risk that we know of and have seen in practice is if the sensors are disconnected by a person.

## Will the sensors and other associated equipment communicate through my building? You may need to tell the supplier what your building is constructed from and how thick walls and floors are.

We offer Rang'R that measures how much coverage you have on a location. If there isn't enough coverage for a sensor to transmit the data to our platform, you can place an additional Gateway to make sure all sensors have coverage and can transmit data to the platform.

## How often does the equipment require replacement batteries or verification?

Our sensors have a battery life of about 2-3 years and (we advise) they need calibration every 3 years to ensure correct, accurate measurements. You could do the calibration and replacement of batteries every 2-3 years at the same time.

## How easy is it to maintain?

Once you've placed the sensors you can just let them hang. Whenever a Clip'R has a low battery or is disconnected, for whatever reason, you will get a notification that the Clip'R is no longer active and that it needs maintenance (calibration, new battery or replacement)

## How can you tell if a sensor is malfunctioning?

We generate a 'reliability score' inside our system. This checks whether sensors are transmitting data, how often they are transmitting data, what temperatures are measured, how much coverage a sensor has and how much battery is still left. Based on these factors we give them a reliability score which pops up beside a sensor in our platform so you can track them in real time.

## How does frequency of measurement affect the battery life?

Every 15 minutes the sensors transmit a measurement to our platform. Based on our findings of the past 4 years we saw that the battery life is about 2-3 years.

## How long will sensors be supported by the supplier, and what happens when they are superseded?

Sensors will always be supported by our system when placed. If they are old and need new hardware they can be easily replaced with another sensor.

# How is the data delivered?

## Is there a time delay between a reading and delivery to the interface?

It takes about 2 hours for the data to be transmitted into the portal. So measurements taken at this moment will be seen 2 hours later in the platform.

## Is data robustly backed up? Where is data stored? Security considerations.

We host our entire infrastructure and platform in the European Economic Area (EEA) in a ISO/IEC 27001 certified datacenter. We encrypt all our client-server communications and data at rest (storage). These measures include secure access for on-premise staff and full end-to-end encryption for both on-site and off-site back-ups.

We use LoRa network technology for our Clip'R sensors and gateways. This means that communication between devices runs on LoRaWAN infrastructure, which we secure using a variety of industry standards for wireless IoT communications and chirp signals. Devices communicate with the remote server over wireless networks, using end-to-end encrypted mobile connections. Find out more about how we encrypt all our communications.

We automatically backup our database every day by creating a snapshot, which allows for rapid recovery in the event of an incident. This automated process never exposes back-ups to external or internal access except to perform a system restore. We save back-ups using encryption and store them at a secure physical location. All the above also applies to file and document back-ups, which we perform weekly.

## What data is provided? All data or high/low/average figures?

Every 15 minutes a temperature is measured and recorded. The system shows all these measurements in a graph and highlights the non-compliances based on the set thresholds.

## How frequently are measurements taken?

Every 15 minutes, all day and night, everyday and night.

## Does data transfer require a cabled network connection to the sensors?

Data is transmitted via the LoRaWAN infrastructure which we secure using a variety of industry standards for wireless IoT communications and chirp signals. Devices communicate with the remote server over wireless networks, using end-to-end encrypted mobile connections. Find out more about how we encrypt all our communications.

## How user friendly is the interface? This is subjective but important.

Our interface is extremely user friendly and increasingly being adopted by LCA/WMSoc members across the UK. Most importantly, unlike other interfaces, ours will take data from sensors and put it to practical use and automaticall interpret data that's why 80% of the legionella consultant in the Netherlands use our software tot digitise legionella control and to automate temperature monitoring.

## Can the interface manipulate data to generate reports? Can it export data in usable formats such as CSV files?

You can export data with our system in a CSV file, but you cannot and will never be able to change or import data into the system. This, to ensure readings by our sensors are correct, accurate and compliant and eliminate the possibility to commit fraud.

## Can the interface generate alerts/non-conformances and how are these managed? Do these meet the requirements of the existing Legionella risk management guidance? Are they user configurable?

You can set certain thresholds and notifications in place to ensure that, if there is a non-compliance, a certain action will be taken. The temperature parameters are configurable so that users can meet the different requirements of different types of buildings (healthcare or normal estates) and types of water (hot, cold, mixed).

## How reliable is data transfer?

We host our entire infrastructure and platform in the European Economic Area (EEA) in a ISO/IEC 27001 certified datacenter. We encrypt all our client-server communications and data at rest (storage). These measures include secure access for on-premise staff and full end-to-end encryption for both on-site and off-site back-ups.

We use LoRa network technology for our Clip'R sensors and gateways. This means that communication between devices runs on LoRaWAN infrastructure, which we secure using a variety of industry standards for wireless IoT communications and chirp signals. Devices communicate with the remote server over wireless networks, using end-to-end encrypted mobile connections. Find out more about how we encrypt all our communications.

## Is data transfer reliant on a customer's own local network and/or internet connection?

No, it's not reliant on a customer's local network since we use LoRaWAN network technology. This means that communication between devices runs on LoRaWAN infrastructure, which we secure using a variety of industry standards for wireless IoT communications and chirp signals. Devices communicate with the remote server over wireless networks, using end-to-end encrypted mobile connections. Find out more about how we encrypt all our communications.

## Can the system be integrated with existing water hygiene management software or building management systems?

It can, but we prefer to use our own management system since our software has certain algorithms in place that will automatically read and interpret data measured by sensors.

## At the end of the contract who owns the data? And can it still be accessed for 5 years from the time of data collection, as required by COSHH?

Data can always be exported from our system and stored in a local or cloudbased drive. It will also be saved in a digital logbook in our system to measure and record all temperature monitoring measurements. These logbooks will be accessible for over 5 years.

# How is the system designed and installed?

## Where will sensors be located and have these decisions been made by those with an understanding of the building water systems installed, the people using these systems, the Legionella risk assessment and the guidance in place?

Our system offers the possibility to have the risk assessment as well as the control scheme in the same place, so the people placing the sensors will always use the underlying risk assessment and control scheme to make decisions. So responsible persons know where the risks are and what control measures need to be performed to ensure a healthy, safe and compliant environment. Based on this information the responsible person can decide if it's necessary to use remote monitoring sensors.

## Are there enough sensors to give a useful thermal profile that informs on the Legionella risk?

yes, as long as you place a high enough volume and in strategically relevant places according to the risk assessment and scheme of controls (i.e. sentinels).

## Will the placement of sensors be prone to damage, vandalism, unintentional switch off, etc.?

Sensors are designed to be able to be taken off a pipe at any time. You can secure this with a form of security e.g. lock, tie-wraps etc. Best is to place them in a spot behind a wall/ceiling to make sure only mechanics can access them.

## Are the sensors invasive/intrusive?

Sensors are non-invasive/intrusive. They can be placed in any spot without causing any damage to the piping system, water flow or whatsoever.

## Do the sensors require access to an external power source to operate?

No, it will run on batteries.

## Who will install the system, are they competent to do so, can you provide evidence for this?

Since we only work with certified legionella consultants, responsible persons and Duty Holders we know who is and isn't certified and thus competent enough to place and install sensors.

## How will the system be commissioned? How will the system be calibrated?

Once the sensors are installed, the system will run automatically; reading and interpreting the data. Every 2-3 years you need to replace the battery and calibrate the sensors to ensure correct, accurate readings.

## Is the supplier able to provide ongoing technical and practical support?

We are able to give ongoing technical support. We have a reactive helpdesk for this that can be called 8:00-17:00 on weekdays, an online Helpcenter that can be accessed anytime, anywhere and we have several Legionella consultants as partners that can help with installation and support online and on-site.

## Who is responsible for training the end user? Both initially and after system upgrades/updates?

Since we sell both via partners (legionella consultants) and direct to duty holders (end users) we are happy to offer training to either group to be competent with our system.

# Security considerations (these may be internal questions or a conversation with the supplier)

## Will this system's communication interfere with other systems on the premises?

Because we use LoRaWAN our sensors will be connected to a completely different system than the normal internet/WiFi connection on the premise. This way we ensure that our data transmission does not interfere with other communication systems.

## Is this type of equipment permitted at my site under the site security conditions?

Depends on the site security conditions, but to give some practical examples we are used by the Dutch Governments, KMPG, NHS premises, and all kinds of different hospitals, care institutions, governmental estates etc.

## How secure is the data transfer, e.g. end-to-end encryption, 2 factor authentication for end user?

**Hosting**

We host our entire infrastructure and platform in the European Economic Area (EEA) in a ISO/IEC 27001 certified datacenter. We encrypt all our client-server communications and data at rest (storage). These measures include secure access for on-premise staff and full end-to-end encryption for both on-site and off-site back-ups.

**Privacy & GDPR**

We physically store all LegionellaDossier data within the European Economic Area (EEA) in full compliance with the EU General Data Protection Regulation (GDPR).

**App communications**

We secure our LegionellaDossier mobile apps in accordance with the best practices for each platform. This includes keeping both iOS and Android apps fully up to date with the latest security features and only allowing apps to communicate with the LegionellaDossier servers using SSL/TLS 1.3 encrypted channels and OAUTH tokens.

**Web communications**

We secure client-server communications using SSL/TLS 1.3 encryption, ensuring data is also encrypted in transit. You can verify this for yourself by checking for the 'lock' symbol and 'https' prefix in your browser's URL field.

**IoT sensors**

We use LoRa network technology for our Clip'R sensors and gateways. This means that communication between devices runs on LoRaWAN infrastructure, which we secure using a variety of industry standards for wireless IoT communications and chirp signals. Devices communicate with the remote server over wireless networks, using end-to-end encrypted mobile connections. Find out more about how we encrypt all our communications.

**Data access**

We store customer data in our database, which remains secure during back-up and in transit.

Our employees only have access to data as part of normal operations and for customer support purposes. We've vetted every individual with access to this data and ensure they follow best practices for handling customer data.

A select group of our employees also has access to our database to ensure operational continuity. We vet these individuals even more stringently and have them sign agreements to ensure they protect all data to which they may have access for operational purposes.

**Backups**
We automatically backup our database every day by creating a snapshot, which allows for rapid recovery in the event of an incident. This automated process never exposes back-ups to external or internal access except to perform a system restore. We save back-ups using encryption and store them at a secure physical location. All the above also applies to file and document back-ups, which we perform weekly.

**Disaster recovery**
Our system administrators have access to all back-ups so they can restore systems to the last-known state in the event of a critical system failure. In such cases, a select group of our employees has access to customer data in order to restore system functionality.

We've also put a disaster recovery plan into place, outlining how to respond in the event of a critical failure. This plan includes several manual steps to ensure data security and rapid recovery.

**Third-party data usage**
LegionellaDossier never shares any customer data between customer accounts and enforces strict data segregation as part of its multi-tenancy SaaS platform policies. This means that no one can access data belonging to another customer without proper authorisation.

Third-party suppliers never have access to customer data, except those with vested business integrations. Our vested partners have access to a very limited dataset, as required for the operational functionality they provide to LegionellaDossier customers. They are not permitted to use this data for any commercial purposes.

# Communication

## What is the best communication method for my application? (WiFi, BLE, NBIOT, low frequency, cellular etc.)

We use LoRa network technology for our Clip'R sensors and gateways. This means that communication between devices runs on LoRaWAN infrastructure, which we secure using a variety of industry standards for wireless IoT communications and chirp signals. Devices communicate with the remote server over wireless networks, using end-to-end encrypted mobile connections. Find out more about how we encrypt all our communications.

## What are the ongoing communication costs?

To use of sensors on the LoRaWAN network consists of different costs, like hardware (sensors) and software (platform). If you want to know more about the costs reach out to our business development team

## What is the network coverage in my area?

An outdoor gateway has coverage up to 1.86 miles. If you place multiple gateways you can expand the coverage if needed.

# Environmental

## How much of the product is recyclable?

The complete case is recyclable and reusable. if there is a hardware error/issues you only have to change the chip inside the sensors the comes out when you change the battery.

## What is the carbon footprint of the supply chain?

No info known

## How does the carbon footprint compare with existing manual monitoring?

No info known

# Financial

## How much does the system cost over its lifespan?
Depends on if you would like to use it temporarily or permanently.

## Lease or purchase? Operational expenditure versus capital expenditure.
We offer both options.

## What are the likely ongoing costs of support?
Cost of support and maintenance are processed in the subscription fee and can be paid for separately when buying sensors as a one-off.

## What does the warranty cover?
Read our terms of service and terms of delivery.

## What is the ongoing cost of access to the software?
To use of sensors on the LoRaWAN network consists of different costs, like hardware (sensors) and software (platform). If you want to know more about the costs reach out to our business development team