Biometric Data Retention and Storage Policy

Berner Food & Beverage Company, LLC requires its hourly employees to clock in and out for their shifts using a biometric system. The biometric information obtained through the use of this system is used to process payroll to Berners' payroll system and/or payroll providers (Paylocity).

Berner Food & Beverage, LLC. in accordance with Paylocity (Berner's HRIS System) shall retain possession of any client's (Berner Food & Beverage, LLC.) employee's biometric data only until the first of the following occurs:

- Paylocity receives written notice of satisfaction from its client, for the initial purpose of collecting or obtaining such biometric data. Such as:
  - The termination of the employee's employment with Paylocity's client.
  - The employee moves to a role within the client organization which does not necessitate biometric data use.
  - The client discontinues the use of Paylocity's product or service which necessitates the use of biometric data.
- Within 3 years of Paylocity receiving written notice of the client's employee's last interaction with the client.
- Temperature Screening data maintenance will continue while the client is active with Paylocity's services and for an additional 7 years for backup purposes.

Biometric data storage is in the cloud which is inaccessible by customers.

- Customers manage and remove Biometric enrollments via the Biometric Dashboard in Time & Labor. The
- cloud stores the following data types:
  - Fingerprints
  - Bitmap images of employee faces
  - Infrared templates of employees
  - The cloud uses random globally unique identifiers (GUIDs) to store data.
    - This allows Paylocity to store the data without any identifying metadata (Names and/or badge numbers).
    - Prevents the ability for a hacker to match the pieces of data to a person, in the event the data becomes compromised.

Paylocity stores Temperature Screening Data within the Time & Labor Management System while the client is utilizing Paylocity's services.

- Paylocity will then store, for backup purposes only, the data for 7 years past the point the client is no longer utilizing Paylocity's services.
- Temperature recordings are not accessible to the managers/supervisors through the time card or the employee profile.
- A company can request Paylocity to create a report of the historical logs of temperature readings. There is
- no purging of this information.
- Clients should review any federal or state-specific requirements that may apply.

HIPAA application to temperature screening:

- HIPAA does not apply to employment records.
  - The Privacy Rule does not protect employment records, even if the information in those records is health related.
  - In most cases, the Privacy Rule does not apply to the actions of an employer.
- If an individual works for a health plan or a covered health care provider: The
  - Privacy Rule does not apply to employment records.
  - The Rule does protect medical or health plan records if the individual is a patient of the provider or a member of the health plan.

Equal Employment Opportunity Commission (EEOC) /ADA

- The EEOC updated the pandemic preparedness guidance in the wake of COVID-19. During a pandemic, it is permissible for an employer to take an employee's temperature and request additional information about any symptoms.
- Under the ADA companies must treat an employee's COVID-19 diagnosis and related medical information as a confidential medical record.
- The Paylocity Biometric Policy provides additional information.

Data Storage Locations include the following:

- Ultima Time Clock device:
  - Employee names and badge numbers (in all scenarios) Schedules for
  - employees with enforced schedules.
  - A subset of Cost Centers / Labor Levels) based upon configuration.
  - Fingerprints (only on clocks with the fingerprint reader enabled)
  - Bitmap images of employee faces and Infrared Templates, used for employee identification (only on clocks with the face module enabled.)

Data stored in the cloud:

- Bitmap images of employee face Infrared templates of employees
- Fingerprints.
- The cloud uses random globally unique identifiers (GUIDs) to store data.
- This allows Paylocity to store the data without any identifying metadata (Names and/or badge numbers). Prevents
- the ability for a hacker to match the pieces of data to a person, in the event the data becomes compromised.

Data stored in Time & Labor:

- Employee names and badge numbers
- Employee schedules
- Cost centers
- The GUIDs to associate the files mentioned above in the cloud to employee badges in Time & Labor. Records of
- when each employee accepts the Biometric Consent agreement.
- The terminal on which the agreement occurs.
- Temperature Screening Data.

Biometric Data Removal:

- Upon receipt of a returned Ultima Time Clock Paylocity will delete any remaining Biometric data from the clock.
  - When a company terminates or inactivates services:
  - Paylocity deletes the associated clocks from the inactive companies. This
  - triggers an immediate reprogramming of the clock.
  - The biometric and user data is deleted from the clock immediately.
  - Associated biometric data and enrollments are deleted from the cloud.
- When an employee terminates or inactivates from the company:
  - The associated biometric data and enrollments are deleted from the cloud.
  - The enrollment data on the associated Ultima Time Clock deletes on the next reprogramming.