BIOSENSE PLATFORM
ORGANIZATION SECURITY AND CONFIDENTIALITY
POLICY AGREEMENT

I. Introduction

A. Purpose of this document

This document will describe the purpose, characteristics of data, user requirements, data uses and the protection of patient identifying information that make up a security and confidentiality policy for the Division of Public Health (DPH) access to the Centers for Disease Control and Prevention (CDC) BioSense Platform. Public health and other staff employed by a state or local organization with a need to access and use BioSense Platform data must read this security and confidentiality and sign the BioSense Platform User Security and Confidentiality Agreement. Protecting the privacy of patients and the security of information contained in the BioSense Platform is a high priority for DPH.

B. Purpose of the BioSense Platform

Pursuant to its public health authority, Wis. Stat. § 250.03(1), with support from the Wisconsin Department of Health Services (DHS), DPH utilizes the CDC's BioSense Platform. BioSense Platform is a nationwide reporting system used for state and federal data reporting and surveillance.

The purpose of this system is to:

- Establish and maintain a nationwide, shared, cloud-based system for reporting and follow-up for syndromic surveillance data.
- Provide alerts to public health authorities and track statewide data.

II. Data Collection

A. Types of data that will be collected

Patient identifying information is maintained in the secure BioSense Platform in order to provide metrics for data categorization and analysis.

Patient identifying information includes:

- County of residence
- Zip code of residence
- Reported age

B. Sensitive data

In addition to reported age, minimal demographic information such as zip code and county will also be collected in order to maintain surveillance activities sufficient to detect any occurrence of syndromes and analyze occurrences, trends, and patterns of public health risks.

C. How the data will be used

The information contained in the BioSense Platform will only be used for the following purposes:

- Support public health surveillance activities
- Generate aggregate outcome data
- Compile and disseminate non-identifying, statistical information on groups of patients or populations in Wisconsin

D. How data will be protected

Sensitive information will be protected through a combined process from CDC and DPH security policies, screening of system users, signed agreements, training, DPH audits, secure passwords, and time-limited access to the system.

III. Access to Data in the BioSense Platform

A. DPH use of the system and audit authority

Patient-identifying information contained in Wisconsin's BioSense jurisdiction will only be accessible to DPH personnel, on a need-to-know basis, including their authorized agents and authorized users. DPH data exchange specialists, administrators, and DHS and/or DPH security and privacy officer(s) and their authorized agents may audit activities on the BioSense Platform to ensure the ongoing security of the data contained therein. Each DPH employee or agent having access to the BioSense Platform will sign a DPH BioSense Platform User Security and Confidentiality Agreement prior to accessing the application.

Local agencies authorized to use the system include:

- Local health departments
- Health care facilities
- Researchers and epidemiologists

B. Local agencies, local administration and how access is granted

Access to the BioSense Platform is limited to public health authorities and their authorized agents. Public health agencies often conduct authorized public health activities with other entities using different mechanisms (e.g., contracts and memoranda or letters of agreement). These other entities are public health authorities with respect to the activities they conduct under a grant of authority from such a public health agency.

The local organizational administrator (LOA) will sign the BioSense Platform Organization Security and Confidentiality Policy Agreement to receive training by the Syndromic Surveillance team on the BioSense Platform organization administration, prior to enrolling other users. The LOA will grant access to local users through an approved access procedure and ensure that users have been adequately trained to use the system and are given only the level of access necessary to perform their assigned duties.

The LOA will maintain a file of signed BioSense Platform User Security and Confidentiality Agreements. We require agreements to be signed by users on an annual basis. If a user changes their employment status, including taking a leave of absence, the LOA will contact the syndromic surveillance team (syndromicsurveillance@wi.gov) immediately. DPH will make updates to user's access as appropriate.

C. Secure and authorized locations and computers

The BioSense Platform use is restricted to computers owned and managed by the user's organization. Location should be restricted to only those places where the organization routinely conducts business or those locations where business is conducted in the event of a public health related emergency. It is the responsibility of the user's organization to ensure that reasonable and prudent security precautions are taken to safeguard confidential information. Examples of reasonable and prudent safeguards for confidential information from the Information Security Forum can be found in the Appendix.

D. Definition of users, categories of users, and how access is granted

If a health care agency wishes to access the BioSense Platform, the BioSense Platform Organization Security and Confidentiality Policy Agreement must be signed by a designated LOA. Only personnel whose assigned duties include functions associated with performing public health activities will be given access to the BioSense Platform data. All personnel, including permanent and temporary employees, contractors, and consultants, who use the BioSense Platform, will be required to sign the BioSense Platform User Security and Confidentiality Agreement before access is granted. Users will receive training at the appropriate access level by the syndromic surveillance team. The LOA will maintain documentation of training.

Each person granted access to the BioSense Platform must have a unique login ID and password. Shared login IDs and passwords will not be permitted. Users are prohibited from disclosing BioSense Platform access codes or protocol to unauthorized persons.

E. Access to the data within the system

The BioSense Platform system contains identifying health information and the data in the system should always be treated in a manner that ensures its safety and confidentiality. Users will be assigned access to personally identifiable data within the system based on jurisdiction. Default user access is restricted to the patients within the user's own jurisdiction and only for data the user has a need to see. Upon mutual agreement, jurisdictions may request the creation of a jurisdictional group to include a group of jurisdictions and specify which users within their agency will be granted access to that group. (A sample jurisdictional group request is included as Appendix 2.) A limited number of users, primarily at the state level, will have access to all Wisconsin jurisdiction data.

If a user does not have access to a particular jurisdiction, the health information will not be visible to the user.

F. Data extracts from the system

Data shall only be exported from the BioSense Platform for public health purposes. Exported datasets shall be de-identified to the extent possible. Users granted permission to export data sets will follow local agency policies related to disposal of data files containing confidential information after they have served their intended purpose.

The use of portable storage devices (e.g., external hard disk drives, flash memory cards such as secure digital and compact flash, solid state storage and MP3 players with storage capacity for holding data, and USB memory sticks) to store downloaded data sets is prohibited unless the device is encrypted. Only encrypted devices that are approved by agency policy may be used. Personal use and sharing of portable storage devices with other staff and external individuals is expressly prohibited.

De-identified datasets will be used to the extent possible. If personal identifying information must be downloaded to a fixed or portable storage device, such devices should be protected by the use of: authentication methods (such as the use of user ID and password, biometrics such as fingerprint scan), access restrictions, encryption techniques (e.g., using encryption software installed on the device, or using encryption software on the workstation, to which the portable storage device connects).

G. Penalties

BioSense Platform data are confidential. Breach of confidentiality requirements and this policy will result in suspension or termination of the user's, health care entity's, or local health department's access privileges to the BioSense Platform and may result in dismissal from employment, civil or criminal penalties for improper disclosure of health information. Periodic audits will be done to ensure compliance with this policy.

IV. Compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

A. About HIPAA

The BioSense Platform system is a CDC program consistent with the data privacy standards established by HIPAA. Balancing the protection of individual health information with the need to protect public health, the Privacy Rule permits disclosures without individual authorization to public health authorities authorized by law to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, public health surveillance, investigation, and interventions.

B. Why DPH is exempt from HIPAA

In the administration of the BioSense Platform, DPH as a public health authority is exempt from the HIPAA requirement defined in section 164.512(b). DPH is not a health plan, health care clearinghouse or health care provider. DPH also does not engage in activities that fall within the HIPAA “business associate” definition set forth in 45 CFR § 160.103.

V. Other Uses of the System and Special Considerations

A. Requests by law enforcement or legal system

Disclosure of information from the BioSense Platform must be in accordance with all applicable state and federal laws. The BioSense Platform data identifying patients will not be disclosed to unauthorized individuals, including law enforcement, without the approval of the DPH administrator.

State responsibility: All subpoenas, court orders, and other legal demands for the BioSense Platform data received by any authorized user of the BioSense Platform must be brought to the attention of the BioSense Platform staff, who will consult DHS legal counsel.

Local responsibility: All subpoenas, court orders, and other legal demands for the BioSense Platform data received by any authorized user of the BioSense Platform must be brought to the attention of the BioSense Platform LOA who will consult with the local organization legal counsel.

B. Research

Requests for data for research purposes that go beyond the scope of the individual provider’s patients or the local health department area of jurisdiction must be forwarded to the DPH administrator for review and approval. State and local organizations using the BioSense Platform data for research purposes must adhere to existing state and federal research provisions and confidentiality laws and statutes.

C. Prohibitions

The BioSense Platform data concerning an identifiable person will not be disclosed without proper and legal authority for purposes other than fulfilling public health obligations. Use of data will be as described in this Agreement.

D. Release of data from the system

Users of the system are only allowed to release data from their own jurisdiction and then only for the purposes of fulfilling public health obligations. This means any numbers/case counts, etc., can only be released when the counts are for the jurisdiction for which the user has authorization.

E. Reporting

The Recipient shall report to DPH within five business days upon becoming aware of any use or disclosure of information not authorized by this Agreement or applicable law.

SIGNATURE PAGE

Check the type of BioSense Platform agency access requested

☐ **Health care provider** ☐ **Public health**

Name of Organization

Name of Main Contact

Street Address, City, and State

Telephone number	Email Address
Name of Signing Authority	Role of Signing Authority

SIGNATURE - Signing Authority

Date Signed

Fax this page to the Office of Health Informatics at 608-266-2584 or mail to:

Division of Public Health
Office of Health Informatics-Syndromic Surveillance
PO Box 2659
Madison, WI 53701-2659

Appendix 1: Relevant sections of Information Security Forum Standards of Good Practice

All workstations (desktop computers or laptops) that will be used to access the BioSense Platform will be encrypted and will have system management tools, access control mechanisms (i.e., to restrict access to the workstation), up-to-date malware protection software to protect against viruses, worms, Trojan horses, spyware, adware, and malicious mobile code; encryption software to safeguard information stored on internal and external hard disk drives, or transmitted by the computer (e.g., using a virtual private network (VPN) when connecting to the agency's network) and automatic time-out after a set period of inactivity, and operating system and applications are patched against known vulnerabilities to help protect you from attack.

Wireless access to the BioSense Platform shall be through local agency wireless access points or connecting to the agency network using a VPN when working in a remote location. Users will take steps to minimize the risks associated with wireless access such as enabling the wireless network interface card only when necessary, using encryption and login IDs and passwords. Wireless access should be authorized, users authenticated, and wireless traffic encrypted. The network should be protected against unauthorized wireless access by using a security "filtering" device (e.g., a firewall or edge server).

Portable devices (e.g., laptop computers and personal digital assistants or PDAs) will be encrypted and protected against theft by providing users with physical locks or equivalent security devices, attaching identification labels, and using indelible marking.

Staff that work in remote locations, including public areas (e.g., hotels, trains, airports, and internet cafes) or from home, should be authorized to work only in specified locations, equipped with the necessary skills to perform required security tasks (e.g., restricting access, taking back-ups, disabling file and folder sharing, and encrypting key files), and made aware of the additional risks associated with remote working (including the increased likelihood of theft of equipment or disclosure of confidential information).

Appendix 2 -- Jurisdictional group request template letterhead

As members of the _____ (*consortium or DPH region or other geographic area*), we request the creation of a BioSense Platform jurisdiction security group that includes the following health department jurisdictions:

List jurisdictions

Users will be assigned to this jurisdictional grouping in accordance with the BioSense Platform Organization Security and Confidentially Policy Agreement.

Sincerely,

Signatures, names, positions