

 C R E D I T • V A L L E Y <small>THE CREDIT VALLEY HOSPITAL</small>	Board Procedure	Board of Directors
TITLE: Whistle Blowing		
DATE OF ISSUE: 2008 02 29	PAGE 1 OF 5	NUMBER: B24.2
SUPERCEDES: N/A	ISSUED BY: Board of Directors TITLE: Chair	

This procedure provides an overview of the ClearView Connects™ whistle blowing solution outlining the various ways in which an employee may submit a report, and the way in which reports can be reviewed by authorized personnel.

1. Reporting Methods

Web Site Reports

When an employee chooses to make a report using the ClearView Connects™ web site reporting system, they enter the ClearView Connects™ home page (www.clearviewconnects.com) from any internet-accessible computer anywhere in the world, enter the organization’s name “CVH” (or however they would identify the hospital) and begin the reporting process. Once they enter the organization’s name, they are immediately taken into a fully encrypted portion of the ClearView Connects™ web application using 128 bit encryption technology (Entrust certificates are used).

Throughout the web site reporting process, no personal information is specifically requested that could identify the reporter. Furthermore, instructions are provided warning the reporter not to divulge any personal information that would identify them if, in fact, they prefer not to be identified. As well, when reports are submitted using the web-based reporting process, the IP address is not recorded in the ClearView Connects™ system. This ensures anonymity for the reporter, and confidentiality of the information provided within the security of the ClearView Connects™ system.

At the conclusion of the reporting session, the ClearView Connects™ system generates a unique login and password for the employee. The system encourages the employee to write this information down and keep it in a safe place, as ClearView DOES NOT keep track of these login and password pairings. This is critical to protect the security of the information in the system, as well as to protect and maintain the anonymity of the employee submitting the report.

Once the report has been submitted, the system immediately generates automatic email notifications and sends these to the authorized Reviewers who have been access to review reports.

Telephone Reports

It is important to first note that the process an employee follows when submitting a report using the telephone hotline (live operator) option is exactly the same as if they were submitting the report themselves using the ClearView Connects™ web-based tool. When an employee chooses to make a report using ClearView's telephone hotline system, they call a special toll free number (1-866-347-7417), and advise the ClearView agent that they wish to make a report. We do not request personal information over the telephone from the employee. Furthermore, instructions are provided warning the employee not to divulge any personal information that would identify them if, in fact, they prefer not to be identified. It is ClearView's policy not to subscribe to caller ID services.

As the employee speaks with the ClearView agent and proceeds to give their report, the ClearView agent enters the report (verbatim) directly into the ClearView Connects™ online reporting system. No separate handwritten notes are taken by the ClearView agent that could be read later by another individual (our call centre is a paperless environment). As information is being entered into the system, it is fully encrypted using 128 bit encryption technology.

At the conclusion of the reporting session, the ClearView Connects™ system generates a unique login and password for the employee. The ClearView agent will provide this login and password to the caller and encourage them to write this information down and keep it in a safe place, as ClearView DOES NOT keep track of these login and password pairings. This is critical to protect the security of the information in the system, as well as to protect and maintain the anonymity of the employee submitting the report.

Once the report has been submitted, the system immediately generates automatic email notifications and sends these to the authorized Reviewers who have been access to review reports.

Voicemail Reports

ClearView recognizes the importance of providing employees with multiple channels through which to report. In other words, the more channels available through which an employee can report, the more comfortable the employee will ultimately feel with the reporting process (in our experience, some employees will be uncomfortable talking to a live third party), and the more likely they will be to use the reporting process to submit important information. We therefore offer a voicemail option (at no additional charge), allowing employees to submit reports by voicemail, in addition to using the live ClearView agent, as part of our hotline protocol. Employees calling the toll free hotline are provided with the choice of speaking with a ClearView agent or leaving a voicemail message containing their report information, which would be transcribed and entered by a ClearView agent directly into the ClearView Connects™ web-based reporting system for review by Credit Valley Hospitals' Reviewers. Unless specifically instructed by the employee who leaves the voicemail message, no personally-identifiable information will be included in the transcribed voicemail report. Note that when an employee submits a report using the voicemail option, there is no further follow up available with the employee, since the voicemail system does not generate and assign a unique login and password for the employee.

Once the report has been submitted, the system immediately generates automatic email notifications and sends these to the authorized Reviewers who have been access to review reports.

Mail Reports

When an employee chooses to make a report by mail, they prepare their information in whatever format they wish. They should be careful to leave out any personal details if they do not wish to be

identified. They may include any documents they feel substantiate the allegations contained in their report. They will mail the report to a confidential ClearView Connects™ Post Office (P.O.) Box. Details about how to submit reports by mail (as well as the other access methods) will be covered in Credit Valley Hospitals' communication program for employees regarding the use of the ClearView Connects™ ethics reporting system. When ClearView receives the report submission by mail, it will be input into the ClearView Connects™ system verbatim, along with any documents that have been attached (these will be scanned electronically and attached to the electronic report). The employee's name will not be included anywhere in the report unless the employee has specifically given authorization for their name to be used. Note that when an employee submits a report using the regular mail option, there is no further follow up available with the employee, since there is no way to communicate a unique login and password to the employee.

Once the report has been submitted, the system immediately generates automatic email notifications and sends these to the authorized Reviewers who have been access to review reports.

Interactive Dialogue Capability

When a report is received by the ClearView Connects™ system, automatic email notifications are immediately sent to all Credit Valley Hospital Reviewers who have access to review that specific category of report (such as Financial Reporting, Theft, Unethical Conduct etc.). The Reviewer can login to the ClearView Connects™ system (using a secure login and 'strong' 8 character password provided by ClearView). After reviewing the report, if there is a desire to ask additional questions of the employee (either to validate the information provided in the report, or to gather additional information to assist in an investigation), the question can be posed within the security of the ClearView Connects™ web application.

When the employee logs back into the system - or calls the toll free hotline (they can do either) - to check the status of their report, they will see that additional information has been requested of them, and will have an opportunity to answer the question(s) if they choose.

We know of no other process, besides this 'virtual' dialogue feature within ClearView Connects™ that provides this on-going important dialogue capability between the employee and Credit Valley Hospital while maintaining the anonymity of the employee. This powerful feature can provide invaluable additional information to investigate reports of wrongdoing that may otherwise never come to light.

2. Reporting and Information Management

The reviewing and reporting capability within the ClearView Connects™ system is extremely robust. Included below is information on the confidentiality of the reports and data storage (including maintaining anonymity) as well as further insight into the reviewing and reporting functionality.

Confidentiality of Reports and Data Storage

Regarding the confidentiality of the reports themselves, reports are kept within the security of the ClearView Connects™ reporting system. This is done specifically to prevent any 'leakage' of information that can occur when information concerning reports is sent by email or by fax, or in some other written form. The ClearView Connects™ solution uses Entrust Secure Sockets Layer

(SSL) 128-bit encryption technology and digital certificates to protect data in transit. Access to the database and operating system permissions are highly restricted.

To further ensure the security and confidentiality of the information in the system, ClearView utilizes a managed firewall service that includes port monitoring and a network intrusion detection service with around-the-clock monitoring of all the TCP/IP traffic. The managed firewall service reviews anomalies in firewall access and looks for access patterns that suggest the possibility of unauthorized access attempts in order to implement new security measures to prevent further access attempts. The network intrusion detection service provides detailed and relevant information regarding security attacks against our servers including what the attacker did, what commands were run, what files were opened and what system calls were executed.

Clearview is also committed to reviewing the security of their server, application and database on an ongoing basis by utilizing the services of outside security experts to perform vulnerability assessments to ensure a security-rich environment. As well, an annual security assessment of their existing information technology (IT) will be performed to identify the strengths and weaknesses and recommend effective security programs consistent with industry-best practices.

Anonymity of the Employee

The anonymity of the employee is maintained and their identity is protected from Credit Valley Hospital Reviewers since personal employee information is never entered into the ClearView Connects™ system, unless the employee specifically provides it when using the web site reporting process, or requests the ClearView agent to include it in the telephone hotline reporting session. ClearView does not subscribe to caller identification services, and all IP address information for web site reports are hashed out and replaced with alias labels. This further protects the identity of employees making reports.

3. Reviewing Functionality

ClearView has established comprehensive reviewing capabilities within the ClearView Connects™ system. Prior to program implementation, ClearView will work with Credit Valley to determine those individuals within the organization who will have responsibility to review each reporting category (Financial Reporting, Theft, Unethical Conflict etc.). There are six (6) Reviewers included in the annual subscription fee (more can be added at an additional charge), and Reviewers can be given access to review multiple categories as needed. It is important to understand that the wider this sensitive information is spread throughout the organization, the greater the likelihood that this information may be "leaked". For internal control purposes, the ClearView Connects™ system has been designed to require a minimum of two (2) Reviewers per category.

When a Reviewer logs in to the ClearView Connects™ system to review reports, they enter a secure login and strong eight (8) character password (containing numbers, letters - upper and lower case, and symbols) that is provided by ClearView. For added security, Reviewer passwords are changed quarterly by ClearView.

One important feature built into the ClearView Connects™ reviewing system is a log tracking capability. Every action taken by a Reviewer or a Reporter within a report is logged with time and date stamps within the report, and a notice of what was done. This provides an accurate record of

all action taken on a report. Examples of actions logged for Reviewers by the ClearView system include:

- Opening a report to review it;
- Entering a comment for other reviewers to read;
- Asking a question back to the employee who has submitted the report;
- Printing a report (there is full print functionality for each report);
- Changing the category of a report (in the event that the employee chose the wrong category);
- Attaching files to the report; and,
- Closing a report.

Examples of actions logged for Reporters (employees) by the ClearView system (and viewable by Reviewers) include:

- Opening their previously-submitted report to review the report status;
- Within this 'Report Status' screen, opening their 'original' report to see how they worded the initial report submission.

Clearview felt it was critical to the integrity of the reports that the system provides a complete audit trail by tracking and logging all report activity. If a specific report were to be investigated, this will provide critical information on what specific actions took place on the report.

The ClearView system also creates an indelible record for each report. These reports, once submitted into the ClearView system, are tamper-proof – they cannot be deleted or changed in any way, by anyone. Information can be appended to the report, but no information can be changed or deleted.

If the external firm determines that no investigation is warranted, this decision will be communicated to the person making the disclosure.