Contents

[1 Introduction 2](#_Toc272338640)

[2 Open Meetings 2](#_Toc272338641)

[2.1 Working Group Meetings 2](#_Toc272338642)

[2.2 Scheduled Conference Calls 2](#_Toc272338643)

[3 Meeting Notifications 3](#_Toc272338644)

[3.1 Unscheduled Meetings 3](#_Toc272338645)

[3.2 Meeting Agenda Notification Timing 3](#_Toc272338646)

[3.2.1 WGM Agendas 4](#_Toc272338647)

[3.2.2 Scheduled Conference Call Agendas 4](#_Toc272338648)

[4 Decision Publication 4](#_Toc272338649)

[4.1 Meeting Minutes 4](#_Toc272338650)

[4.2 Electronically Recording Meetings 5](#_Toc272338651)

[5 Quorum Requirements 5](#_Toc272338652)

[5.1 Preponderance of Interest 5](#_Toc272338653)

[5.2 Presiding Chair Vote 5](#_Toc272338654)

[6 Decision Threshold Requirements 6](#_Toc272338655)

[6.1 Revisiting Decisions 6](#_Toc272338656)

[7 Electronic Voting 7](#_Toc272338657)

[8 Proxy Participation 7](#_Toc272338658)

[8.1 Proxy Not Allowed 7](#_Toc272338659)

[8.1.1 Statement of Position 7](#_Toc272338660)

[9 Roberts Rules of Order 8](#_Toc272338661)

# Introduction

1. This document is the Security Work Group decision-making practices (DMP) for Health Level Seven (HL7) Security Work Group, and is adapted from the generic HL7 Work Group DMP which applies to all WGs. The Security Work Group will adhere to a set of decision-making practices that ensure consensus, openness, and balance of interest.
2. Balance of interest is related to normative ballot procedures; refer to HL7 Essential Requirements: Due process requirements for HL7 American National Standards (HL7 ER) for additional information on normative ballots and balance of interest. §01.03 presents the ANSI position; while §02.03.03 presents the HL7 process for seeking balance in normative ballot consensus groups.
3. The practices as outlined in this document are designed to enable timely decision-making balanced with an earnest attempt to ensure that input from all affected parties is considered. The decision-making practices are intended to govern the standard operating procedures of HL7 WGs and Committees and not intended to conflict with rules governing ballot procedure as defined by ANSI, the HL7 Governance and Operations Manual (GOM) and the HL7 ER.
4. In the event of joint meetings, the DMP of the host WG shall be the governing document.

# Open Meetings

1. Security Work Group meetings and conference calls are open to all interested parties.
2. The purpose of these Security Work Group meetings and calls is to transact business including the resolution of design and implementation issues related to the Security Work Group’s area of responsibility and to make decisions relevant to Security Work Group business.
3. Meetings of the Security Work Group are open to everyone to ensure that viewpoints of all affected parties have an opportunity to be shared and considered. Everyone will be given an opportunity to speak; however, the chair may limit discussion on topics deemed to be non-constructive.
4. Depending on the purpose or mode of the meeting certain participants are expected to attend.
5. Other HL7 members may be asked to attend to provide specific input regarding a particular issue.
6. Guests (non HL7 members) are welcome to participate in the Security Work Group and are recognized as guests of HL7.
7. In keeping with the ANSI policy on openness, Guests may participate on all matters related to the development of HL7 protocol specifications.

## Working Group Meetings (WGM)

1. Security Work Group sessions during Working Group Meetings (WGM) may be attended by any registered WGM attendee who wishes to participate.
2. Participants should introduce themselves and identify the nature of their affiliation with HL7 or, if non-members, their particular interest in the agenda items being addressed.

## Scheduled Conference Calls

1. Scheduled or periodic conference calls may be attended by persons registered on the Security Work Group list server.
2. Persons not subscribed to the Security Work Group list may still attend, however, all meeting announcements, minutes, and other notices will be sent to the list and posted to the Security Work Group web page or wiki (see Section 3). Therefore anyone expecting to participate is encouraged to join the list so that the Security Work Group can communicate with them.

# Meeting Notification

1. All activities shall be conducted in public view with efforts made to ensure ample notification of those interested. The Security Work Group shall utilize the following key mechanisms to notify interested parties of its activities
2. Security Work Group listserv <http://www.hl7.org/Special/committees/secure/listserv.cfm>
3. Security Work Group web page under <http://www.hl7.org/Special/committees/secure/index.cfm>
4. Security Work Group wiki page under <http://wiki.hl7.org/index.php?title=Security>
5. Satisfaction of minimal notification requirements dictates that relevant announcements and supporting materials are posted to ***both*** the listserv and the web or wiki page.
6. The listserv (and/or wiki) will be used predominantly for discussion threads, notifications, and draft documents; whereas the web page will be used predominantly for final documents and document resources (decision documents, minutes, papers, etc.)
7. Any use of the terms **post**, **posted**, or **posting** refers to notification, subject to the above constraints.

## Unscheduled Meetings

1. The Security Work Group requiring face-to-face meetings between scheduled WGM sessions or calls have two options:
2. An 'Out of Cycle Meeting' can be convened as defined in GOM §11.04, given at least a 30-day notice.
3. The issues may be discussed in an informal group, bringing forward recommendations to the list or as a discussion topic for the next regularly scheduled WGM session or conference call. Recommendations brought forward by the informal group are not binding decisions until acted upon by the Security Work Group in regular session or conference call conforming to the notification requirements defined in Section 3.

## Meeting Agenda Notification Timing

1. Meeting notification and the proposed agenda are provided prior to the meeting.
2. Binding decisions can be made only at meetings with the required advance notification where quorum is met;
3. A **binding decision** refers to any decision made by the Security Work Group that establishes a practice, formal recommendation, or formal action by the Security Work Group (e.g., creating a new program, rendering guidance, etc.).
4. The co-chairs of the Security Work Group shall make every attempt to ensure that all parties with an interest in agenda topics are made aware of the meeting time and location subject to the documented notification requirements. As appropriate, Security Work Group activities will be cross-posted to other HL7 lists, depending upon the topic and type of meeting as indicated in the following list. The GOM stipulates that all face-to-face meetings require at least a 30-day notice.

### WGM Agendas

1. WGM Security Work Group session schedules are posted in the meeting brochure; specific Security Work Group agendas are posted under work group meeting information at the HL7 wiki (wiki.hl7.org/index.php?title=WGM\_information)
2. A preliminary agenda is developed by the end of the prior WGM and posted with the minutes following the WGM (posting deadlines are established by HL7 Headquarters; typically 2 weeks after the WGM).
3. The preliminary agenda is finalized at least two weeks prior to the WGM and posted within 2 business days or as required by HL7 Headquarters.
4. Recognizing the dynamic nature of the WGM, the agenda may require updates. Notification will be satisfied so long as at least two of the following are used:
5. E-mail notification by 6:00 pm local time the evening before the event
6. Notification on the bulletin board (near the HL7 registration desk) at least 2 quarters (there are four 90-minute quarters per WGM day) prior to the event
7. Announcement during the general session or lunch session prior to the event

### Scheduled Conference Call Agendas

1. Scheduled Conference Call Agendas shall be posted by close-of-business of the first business day prior to a call.
2. Preliminary agendas for the next conference call are to be determined at the close of each teleconference.

# Decision Publication

## Meeting Minutes

1. Minutes will be produced and published for all WGM sessions and conference calls achieving quorum.
2. The presiding co-chair of the meeting is responsible for ensuring that minutes are taken and posted.
3. Where quorum is not achieved, the production of minutes is at the discretion of the presiding co-chair.
4. Minutes shall include, at a minimum, the following information:
5. Date, time and location of the session/call
6. List of attendees including names and organizations
7. Identification of presiding chair (if the presiding chair changes during meeting this should be noted in the minutes)
8. Assertion of quorum (met or not met)
9. A summary of discussion topics and the outcome of proposals or motions made (including vote tallies if votes were taken)
10. Minutes shall be published on the Security Work Group webpage or the wiki as well as the Security Work Group listserv.
11. Minutes from a WGM shall be posted 2 weeks after the WGM; minutes from a conference call will be posted within one week following the call.

## Electronically Recording Meetings

1. The Security Work Group may decide that they wish to electronically record a session, conference call or Security Work Group event including audio or video recordings.
2. Electronic recordings will not replace the minutes or the requirements for minutes as defined in Section 4
3. Prior to starting any electronic recording, the chair will seek approval from all attendees for the recording to occur and will note the acceptance by all attendees in the meeting minutes.
4. With the approval of the Security Work Group to proceed with any electronic recording, the chair will explain the method and purpose of the recording and how the recording will be used and made available.

# Quorum Requirements

1. A quorum for Security Work Group meetings require that a co-chair and at least two other Security Work Group members be present, where no single organization or party represents more than a simple majority of the voting Security Work Group members present.

[NOTE: The minimum number of attendees required for a quorum varies based on Security Work Group size, but SHALL be no less than two in addition to the presiding chair.

1. A motion may be made, by any participant, to defer major decisions even if quorum is met, particularly if key stakeholders are not present.

## Preponderance of Interest

[NOTE: The following section is suggested. WGs that routinely face controversial decisions that are influenced by organizational participation should consider rigid enforcement. Those that do not should consider “only-as-needed” enforcement.]

1. To ensure balanced committee decision-making, no single organizational interest may wield a “Preponderance of Influence” within a Work Group.
2. Preponderance of Influence is defined as having one organization representing more than 50 percent of the voting Security Work Group members in session.
3. This rule may be either stringently or loosely enforced, at the discretion of the presiding chair, given that the presiding chair is not a member of the organization in question. However, if a Security Work Group member believes that decisions are being significantly influenced, he/she may invoke the “Preponderance of Influence Clause” requiring the co-chair to bring the voting membership into compliance with this 50% rule. This invocation is non-debatable.

## Presiding Chair Vote

1. The presiding chair may cast a vote in only two circumstances:
2. The presiding chair may cast a tie-breaking vote.
3. The presiding chair may vote when that vote corrects potential preponderance of influence concerns within the Security Work Group.
	1. For example: 5 members are present, one of whom is the presiding chair. Two others are with the same organization; the co-chair’s vote removes the majority vote of the over-represented organization and thus brings the committee into balance.
4. In all circumstances, the Security Work Group can have no more than one presiding chair, with any other co-chairs participating as regular members when not presiding.
	1. Note that the presiding chair can change within the course of a given session so long as a public statement recognizing the change is made and recorded in the minutes.
5. Although any issue may be discussed at any time, binding actions cannot be taken without sufficient notification (see Section 3) and quorum (see Section 5). Absence of either of these conditions allows the Security Work Group to issue recommendations that must subsequently be ratified by the Security Work Group subject to satisfying constraints placed upon binding decisions.
6. No co-chair should preside over discussions or vote for which they could reasonably be perceived to have a vested interest.

# Decision Threshold Requirements

1. The Security Work Group will strive for consensus in decision-making; however, decisions of the Security Work Group are affirmed by simple majority.
2. While decisions are affirmed by simple majority, the Security Work Group shall endeavor to make its decisions via a consensus process.
3. Where a consensus decision is not reached the Security Work Group shall agree on a course of action to be followed in order that sufficient information to achieve consensus may be gathered.
4. To be called a consensus decision, it must receive two-thirds (66%) majority support. A variety of informal techniques may be used to determine if consensus may be reached including, but not limited to, straw poll, Robert’s Rules of Order, seeking response to a hypothetical opposing view, and polling each participant to voice their position on the issue.
5. When a formal vote is taken, the co-chair will explain the eligibility for voting.
6. Any participant concerned that a given organization has undue representation or influence within a session of the committee may invoke the “Preponderance of Influence” clause (see Section 5.2). This invocation is non-debatable.

## Revisiting Decisions

1. It is recognized that revisiting previously made decisions inhibits progress and should be discouraged. That said, circumstances might exist that warrant re-opening discussion on a previously resolved issue.
2. To dissuade this practice, such re-opening requires a formal motion, second, and two-thirds (66%) majority affirmative vote subject to the quorum rules in this document.
3. In order for the decision to revisit a previous decision to be considered binding, advance notification as specified in Meeting Notifications (section 3) is required.
4. The Meeting Notifications (section 3) can be waived to expedite ballot reconciliation items if the Security Work Group determines that the new discussion represents the same range of views as addressed in the original decision.

# Electronic Voting

1. Some decisions considered outside of the WGM may be resolved electronically.
2. Security Work Group electronic votes will be announced on the Security Work Group list server.
3. If the motion was NOT made, seconded and discussed during a quorum meeting then, the workgroup will circulate the motion and request a second via the list service. Once seconded there will be a period of not less than 3 days of discussion via the list server prior to the opening of the e-vote.
4. The Security Work Group electronic votes will be held open for a minimum period of 1 week but may be longer. The voting period will be defined in the announcement of opening the e-vote.
5. Quorum for electronic voting will be set at 90% of the number of attendees at the last session or call in which quorum was achieved. Quorum shall be at a minimum the same as for a Security Work Group session or call as defined in Section 5.
6. If quorum has not been achieved at the end of the announced voting period, the vote will be closed as unsuccessful due to lack of quorum.
7. Electronic votes are decided by simple majority of the affirmatives and negatives.

# Proxy Participation

## Proxy Not Allowed

1. The Security Work Group recognizes that competing interests sometimes prohibit a member’s ability to participate in person at all meetings. However, in the interest of encouraging the dynamic exchange of ideas, the Security Work Group does not endorse/allow participation by proxy.
2. If an organization feels strongly enough about a particular topic to want to participant in the vote, that organization shall send adequate representation. Where possible, the co-chairs should accommodate schedules to ensure such representation can be present in the appropriate venue.

### Statement of Position

1. Those wishing to establish a position in writing may do so subject to the notification requirements outlined in Section 3
2. Statements of Position received prior to or during the meeting will be shared by the co-chair as part of the discussion on the related topic.
3. The presiding chair has the responsibility to present these positions during relevant discussion, though they are not under any obligation to support or defend them.
4. These statements do not carry the weight of a vote and are included as informational only for consideration by the committee.
5. All Statements of Position received in electronic form will be included as attachments to the minutes.

# Roberts Rules of Order

1. The Security Work Group shall rely upon Roberts Rules of Order in the event that formal guidance of parliamentary procedure is needed or requested.
2. In the interest of ensuring the effective and active engagement of all participants, the Security Work Group shall follow its documented decision-making practices, referring to Roberts Rules of Order in the event of a question or concern. Since Robert’s Rules of Order provides formalism for addressing almost all matters of process, this provides a “backup mechanism” of formality in the event that it is required.
3. It is the responsibility of the presiding chair to guide the Security Work Group to an efficient and effective outcome. The Security Work Group shall follow, in this order of precedence, these Decision-making Practices (which cannot conflict with the Bylaws, GOM or HL7 ER), the GOM, the HL7 ER, the Bylaws, and Roberts Rules of Order. The established decision-making practices can refine certain policies and procedures so long as they remain in accordance with the GOM, HL7 ER and Bylaws.
4. In the event that an issue arises where formality is required and no other guidance exists, Robert’s Rules of Order shall take precedence. This provides a “common denominator” to keep in-check the power of the presiding chair and to confirm the rights of all participants and members.

|  |
| --- |
| Document Revision History |
| Version Number | Adoption Date |
| 3.0 | January 1, 2011 |
| 4.0 | May 1, 2014 |
| 4.1 Adapted specifically for Security Work Group | September 18, 2014 |